Defence Research and Development Canada
Recherche et développement pour la défense Canada

Major Events Coordinated Security Solutions Technical Report Closeout (MECSS)

The Application of Science and Technology to Reduce Risk for V2010 and G8/G20 Summits

Colin Murray
Donna Wood
Paul Chouinard
Lynne Genik
Jane MacLatchy
Murray Dixson
Patrick Dooley
Ron Funk
Adel Guitouni
Tony Masys
Ted Sykes

Defence R&D Canada – CSS

Technical Report
DRDC CSS TR 2010-13
December 2010

Canada

Major Events Coordinated Security Solutions (MECSS)

The Application of Science and Technology to Reduce Risk for the Vancouver 2010 Winter Olympics and Paralympics and the G8/G20 Summits

Colin Murray, DRDC CSS
Donna Wood, DRDC CSS
Jane MacLatchy, RCMP
Paul Chouinard, DRDC CSS
Murray Dixson, DRDC CSS
Patrick Dooley, DRDC CORA
Ron Funk, DRDC CORA
Lynne Genik, DRDC CSS
Adel Guitouni, DRDC Valcartier
Tony Masys, DRDC CSS
Ted Sykes, DRDC CSS

Defence R&D Canada – CSS

Technical Report
DRDC CSS TR 2010-13
December 2010

Principal Author

Original signed by Donna Wood

Donna Wood

Project Manager MECSS

Approved by

Original signed by Colin Murray

Colin Murray

Project Director MECSS

Approved for release by

Original signed by Mark Williamson

Mark Williamson

Chairman DRDC CSS Document Review Panel

This work was conducted under the Major Events Coordinated Security Systems (MECSS) project number 33bd a project under the Public Security Technical Program and managed by the DRDC Centre for Security Science. Sponsors for this project included the RCMP Major Events Section, V2010 Integrated Security Unit, BC Integrated Public Safety, Canadian Forces Joint Task Force Games and Public Safety Canada Government Operations Centre

Abstract

The Major Events Coordinated Security Solutions (MECSS) project was a multi-agency collaborative partnership established to reduce the security risk associated with the Vancouver 2010 Winter Olympics and Paralympics (V2010) and the G8/G20 Summits. Decision support, exercise support, reach-back scientific advice and deployed support during the V2010 and Summits was provided in the following domains: Command and Control, Chemical Biological, Radiological, Nuclear and Explosives, Critical Infrastructure, Surveillance, Physical Security, Cyber and Psycho-Social. This technical report constitutes the closeout report for the MECSS project and provides a summary of the results achieved by MECSS.

Résumé

Le projet Solutions concertées pour la sécurité des grands événements (SCSGE) était un partenariat de collaboration multi-organismes, mis en place afin d'atténuer les risques pour la sécurité des Jeux olympiques d'hiver de Vancouver 2010 et des sommets du G8 et du G20. Il a permis de fournir l'aide à la décision, le soutien des exercices, les conseils scientifiques extérieurs et le soutien aux opérations de déploiement durant les Jeux olympiques et ses sommets dans les domaines connexes au commandement et contrôle, aux incidents chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRNE), aux infrastructures essentielles, à la surveillance, à la sécurité physique, à la cybernétique et à la socio-psychologie. Le présent rapport technique clôture le projet SCSGE et fournit un résumé des résultats atteints

This page intentionally left blank.

Executive Summary

Major Events Coordinated Security Solutions Technical Report Closeout: The Application of Science and Technology to Reduce Risk for V2010 and G8/G20 Summits

Colin Murray; Donna Wood; Jane MacLatchy; Paul Chouinard; Murray Dixson; Patrick Dooley; Ron Funk; Lynne Genik; Adel Guitouni; Tony Masys; Ted Sykes; DRDC CSS TR 2010-13; Defence R&D Canada – CSS; December 2010.

Introduction or background: The Major Events Coordinated Security Solutions (MECSS) project was a multi-agency collaborative partnership, established to reduce the security risk associated with the Vancouver 2010 Winter Olympics and Paralympics, and the G8/G20 Summits. MECSS was implemented as a formal project within the Public Security Technical Program (PSTP), under Defence Research and Development Canada (DRDC) management through the Centre for Security Science (CSS).

Results: MECSS enabled support to the following security partners: RCMP Major Events Section, V2010 Integrated Security Unit, BC Integrated Public Safety, Canadian Forces Joint Task Force Games, and Public Safety Canada. Decision Support, Exercise Support, Reach-back scientific advice and deployed support during the V2010 and G8/G20 Summits was provided in Command and Control, Chemical Biological, Radiological, Nuclear and Explosives, Critical Infrastructure, Surveillance, Physical Security, Cyber and Psycho-Social. The MECSS project produced more than 195 scientific reports, reflecting the effort, dedication and professionalism of more than 180 scientists, technologists, and others from across DRDC and other federal Departments and Agencies.

Significance: Post event reports are providing a growing bank of evidence to demonstrate the degree to which science and technology was able to contribute to the overall reduction of security risk associated with V2010. This experience and the subsequent momentum, will lead to a stronger institutionalized approach in the way Canada will exploit science and technology to address future safety and security challenges. This is a significant and progressive shift, which will enhance Canada's overall national resilience.

Future plans: Work will continue under the DRDC CSS to provide operational Science and Technology support to our security partners. In particular, the Major Events Framework will continue to add valuable content, Science Town will evolve with its partners and scientific advice will always be available through reach-back.

Sommaire

Solutions concertées pour la sécurité des grands événements : Application de la science et de la technologie afin d'atténuer les risques pour les Jeux olympiques et paralympiques d'hiver de Vancouver 2010 ainsi que pour les sommets du G8 et du G20

Colin Murray; Donna Wood; Jane MacLatchy; Paul Chouinard; Murray Dixson; Patrick Dooley; Ron Funk; Lynne Genik; Adel Guitouni; Tony Masys; Ted Sykes; DRDC CSS TR 2010-13; R & D pour la défense Canada – CSS; Décembre 2010.

Introduction ou contexte : Le projet Solutions concertées pour la sécurité des grands événements (SCSGE) était un partenariat de collaboration multi-organismes, mis en place afin d'atténuer les risques pour la sécurité des Jeux olympiques et paralympiques d'hiver de Vancouver 2010 ainsi que pour les sommets du G8 et du G20. Les SCSGE ont été mises en œuvre en tant que projet officiel dans le cadre du Programme technique de sécurité publique (PTSP), sous la coordination de Recherche et développement pour la défense Canada (RDDC), par l'intermédiaire du Centre des sciences pour la sécurité (CSS).

Résultats : Le projet SCSGE a permis d'appuyer les partenaires suivants en matière de sécurité : Section de services de protection des événements majeurs de la GRC, Groupe intégré de la sécurité de Vancouver 2010, Équipe intégrée de sécurité publique de la C.-B., Force opérationnelle interarmées des Forces canadiennes pour les Jeux olympiques et Santé publique Canada. Il a permis d'offrir l'aide à la décision, le soutien des exercices, les conseils scientifiques extérieurs et le soutien aux opérations de déploiement durant les Jeux olympiques et les sommets dans les domaines connexes au commandement et contrôle, aux incidents chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRNE), aux infrastructures essentielles, à la surveillance, à la sécurité physique, à la cybernétique et à la socio-psychologie. Dans le cadre du projet SCSGE, on a produit plus de 195 rapports scientifiques, fruit des efforts, du dévouement et du professionnalisme de plus de 180 scientifiques, technologues et autres professionnels de RDDC ainsi que d'autres ministères et organismes fédéraux.

Importance : Les rapports rédigés à la suite de cet événement démontrent de plus en plus à quel point la science et la technologie ont permis d'atténuer de façon générale les risques pour la sécurité des Jeux olympiques. Cette expérience et cet élan donneront lieu à une approche institutionnalisée plus solide quant à la façon dont l'État fera appel à la science et à la technologie pour résoudre les problèmes de sécurité qui se poseront. Il s'agit d'un changement d'avant-garde important qui, selon moi, augmentera la résilience générale de la nation canadienne.

Recherches futures : Le CSS de RDDC poursuivra les recherches afin de fournir le soutien scientifique et technique aux opérations de nos partenaires en matière de sécurité. Plus particulièrement, la Structure de sécurité pour les grands événements continuera d'accumuler des contenus précieux, le « village scientifique » continuera de progresser en collaboration avec ces partenaires, et des conseils scientifiques seront toujours disponibles par le truchement de l'appui extérieur.

Table of contents

Abstract ……. i
Résumé ……..... i
Executive Summary..... iii
Sommaire iv
Table of contents v
List of Figures vii
List of tables viii
Acknowledgements ix
1 Overview..... 1
1.1 Background and History..... 1
1.2 Mandate and Activities..... 1
1.3 Achievements 3
1.3.1 Pre-deployment 4
1.3.2 Deployment..... 5
1.3.3 Legacy..... 6
1.3.4 Conclusion 6
2 Technical Performance 7
2.1 Scientific Advisor Joint Task Force Games 7
2.2 Scientific Advisor V2010 Integrated Security Unit..... 9
2.3 Scientific Advisor Integrated Public Safety 12
2.4 Scientific Advisor Royal Canadian Mounted Police..... 13
2.5 CBRNE Domain Lead..... 14
2.6 Command and Control Domain..... 17
2.7 Critical Infrastructure Domain 20
2.8 Exercise Domain 22
2.9 Surveillance Domain 27
2.9.1 Marine 27
2.10 Psycho-social Domain..... 29
2.11 Physical Security 29
2.11.1 Software-Based Model & Tool Development..... 30
2.11.2 Short-Deadline Analysis 31
2.11.3 Experimentation & Field Trials. 32
2.11.4 Deployed Games-Time Support (February, 2010)..... 32
2.12 Cyber 33
2.13 Major Events Security Framework..... 35
2.14 V2010 Deployment 36

2.15 G8/G20 Support ... 37
2.16 Schedule Performance Summary ... 38
2.17 Cost Performance Summary ... 38
2.18 Leveraged Activities ... 39
3 RECOMMENDATIONS FOR FOLLOW-ON ACTIVITY ... 41
3.1 Transition of Project Products into Operations ... 41
3.2 Follow-On R&D Projects Recommended ... 42
3.3 Intellectual Property Disposition ... 43
3.4 Disposition of Project Products ... 44
3.5 Policy or Procedural Changes ... 45
4 LESSONS LEARNED SUMMARY ... 47
4.1 Project Director's Observations ... 47
4.1.1 Strategic Considerations ... 47
4.1.2 Set-up ... 49
4.1.3 Execution ... 50
4.1.4 Legacy ... 50
4.2 Project Manager's Observations ... 52
4.3 Exploitation Officer's Observations ... 54
4.3.1 Exploitation Opportunities ... 54
4.3.2 RCMP Engagement ... 61
4.3.3 Cultural Challenges: RCMP and DRDC ... 61
4.4 Comments on Project Assumptions, Constraints and Risk Factors ... 62
4.4.1 Assumptions ... 62
4.4.2 Constraints ... 62
4.4.3 Risks ... 62
4.5 After Action Review ... 63
4.5.1 Best Practices ... 63
4.5.2 Challenges ... 65
4.5.3 Recommendations ... 65
5 MECSS Reports ... 67
List of Acronyms ... 84

List of Figures

Figure 1: MECSS Domains 2
Figure 2: MECSS Delivery Model 3
Figure 3: (A) Multi-Layered Operations: (B) Three Pillars with Multi-Stakeholders 17
Figure 4: MECSS Legacy 51

List of tables

Table 1 : Milestones 38
Table 2: Original Cost Breakdown - approved 5 May 2008 38
Table 3: Revised Cost Breakdown - approved 6 Apr 2010 39
Table 4: Actual Cost breakdown 39
Table 5: Leveraged Activities 40

Acknowledgements

One of the successes of the Vancouver 2010 Winter Olympics is the degree to which Science and Technology (S&T) was able to contribute in the mitigation of security risk. Many organizations and individuals played a significant role in facilitating the extent to which S&T was engaged. The RCMP Major Events Section warrants special recognition for their vision, and the degree to which they were able to create the conditions for S&T expertise to be accepted within the policing community. As well, Lieutenant Colonel Pat Koch is recognized for his leadership in championing S&T support within the Integrated Security Unit. Acknowledgement is extended to the BC Integrated Public Safety team, who proactively embraced opportunities to use S&T in addressing some of the more pressing safety and security concerns. As well, the ISU leadership is recognized for their willingness to accept non-traditional support from outside the policing community. Strategically, the Privy Council Office, Office of the Coordinator for 2010 Olympics and G8 Security was instrumental at enabling support for S&T participation from across Federal Departments and Agencies. Finally, special appreciation is extended to the hundreds of scientific staff from across Canada, who demonstrated incredible dedication and passion in delivering S&T support to the security operations for the Vancouver 2010 Winter Olympics and Paralympics, as well as the Huntsville G8 and the Toronto G20.

Contibuting authors: J. Maclatchy, M. Dixson, P. Dooley, A. Guitouni, T. Sykes

This page intentionally left blank.

1 Overview

1.1 Background and History

Science and Technology support to the Vancouver Winter Olympics began in 2005. Initially it focused on an experimental thrust that included the Department of National Defence (DND), Canadian Forces Experimentation Centre (CFEC), Canada Command (CanadaCOM), Defence Research and Development Canada and the RCMP. Much of this effort was packaged within an experimental campaign plan called Pegasus Guardian (PG). This activity served as a central coordination point for various S&T activities, which could contribute to the challenges associated with inter-agency coordination of Major Events security. Joint Command Decision Support for the 21st Century Technology Demonstration (JCDS21 TD) is an example of the type of S&T effort that was leveraged in support of V2010. In 2007, a full scale experiment called PEGASUS GUARDIAN I was held in British Columbia that served to unite many of the S&T activities, as well as the key players responsible for V2010 security planning. This work allowed the V2010 Integrated Security Unit (ISU) to develop and test its initial processes under controlled conditions.

The parallel work of CFEC and JCDS21 experiments at PG provided an early opportunity for the ISU/JTFG staffs to become acquainted with the framework of operationally relevant scenarios, and familiar with each other. It was also a critical event in the initiation of MECSS as a project because it was the juncture at which leadership from the Privy Council Office (PCO), the RCMP, and DRDC discussed the opportunity for an integrated approach to federal S&T.

In December 2007, the CEO DRDC directed that a project be created to coordinate federal science and technology in support of the V2010 security partners. The Director General from DRDC CSS was appointed as the Project Leader. A Senior Review Board (SRB) was created that included representation from the ISU, RCMP Major Events and Protective Policing Directorate, Canada Command, the Province of British Columbia, and DRDC. Later, representation was added from the Operations Directorate within Public Safety Canada. The Project took ownership of the ongoing activities, much of which had been generated through the Canadian Forces Joint Task Force Pacific (JTFP) Operational Research Team (ORT) leader, who had established a presence in the V2010 ISU. The Project then set out to develop a delivery model that would build on existing work and relationships within the security partnerships, and facilitate the opportunity for S&T contributions. The Project was named Major Events Coordinated Security Solutions (MECSS), and the Project Synopsis Sheet was signed in May 2008. In the period between receiving direction from the DRDC Chief Executive Officer (CEO) and the formal project approval in May 2008, work continued on the ground in direct support of the security partners. A number of operational research scientists played a critical role in addressing their priority needs and in building the trusted relationships that were the foundation of work that would follow.

1.2 Mandate and Activities

The MECSS Project was a multi-agency collaborative partnership, established to reduce the security risk associated with V2010 and the G8/20. MECSS was implemented as a formal project

within the Public Security Technical Program (PSTP), under DRDC management through the Centre for Security Science (CSS). The objectives of the MECSS project were to:

a. Assist the functional authorities in reducing the security risk associated with V2010 and the G8/20 through the coordinated application of science and technology, and

b. Contribute to the establishment of an enduring Major Event security architecture that can be applied to future Major Events in Canada.

MECSS was created to coordinate, when appropriate, S&T activities to ensure the timely delivery of effective capabilities that meet the operational needs. Typical program activities within the scope included:

a. Decision support;

b. Operational analysis;

c. Deployed S&T capabilities;

d. Federal S&T Reach-back; and

e. Exercise/validation of security and safety capabilities.

The work conducted within this project was grouped into domains of expertise. It was recognized that much of the work conducted under MECSS would cross each domain and include a broad spectrum of activity. The domains, as per Figure 1, were established primarily to facilitate coordination and collaboration, and to provide some clarity to the scope of work that would be conducted.

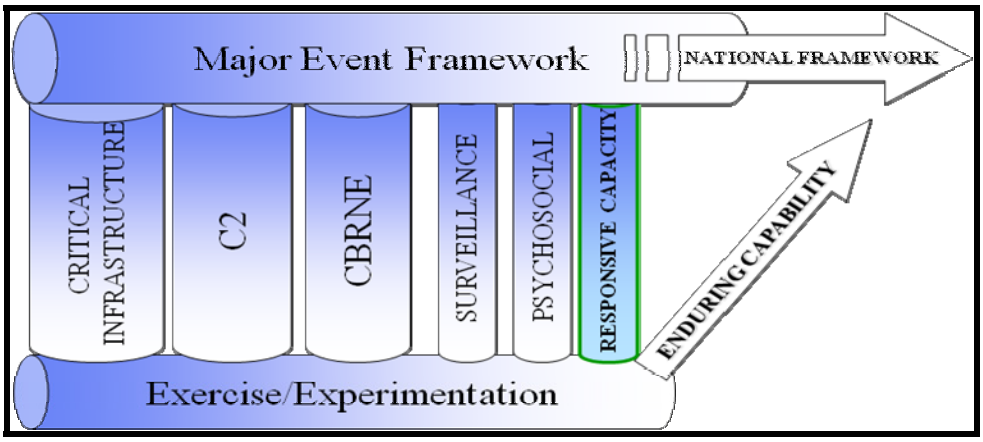

Figure 1: MECSS Domains

The MECSS Delivery Model was born of the philosophy that S&T is best delivered into the operational community through the integration of scientific advisors (SA) into the key decision loops within the security partner organizations. Embedded SAs offered the MECSS team insight

into the Operators' most pressing security and safety challenges. The SAs primary responsibilities included:

a. Establish trusted links within host organization;

b. Coordinate/provide timely and relevant S&T advice and expertise, including the coordination of reach-back as required;

c. Identify operational challenges suited to S&T solutions;

d. Facilitate the generation and transfer of knowledge;

e. Provide direct support to specific projects; and

f. Maintain active liaison within the SA network.

The model at Figure 2 illustrates how MECSS was postured to broker S&T contributions from amongst a broad spectrum of S&T delivery organizations, in support of the primary security delivery organizations.

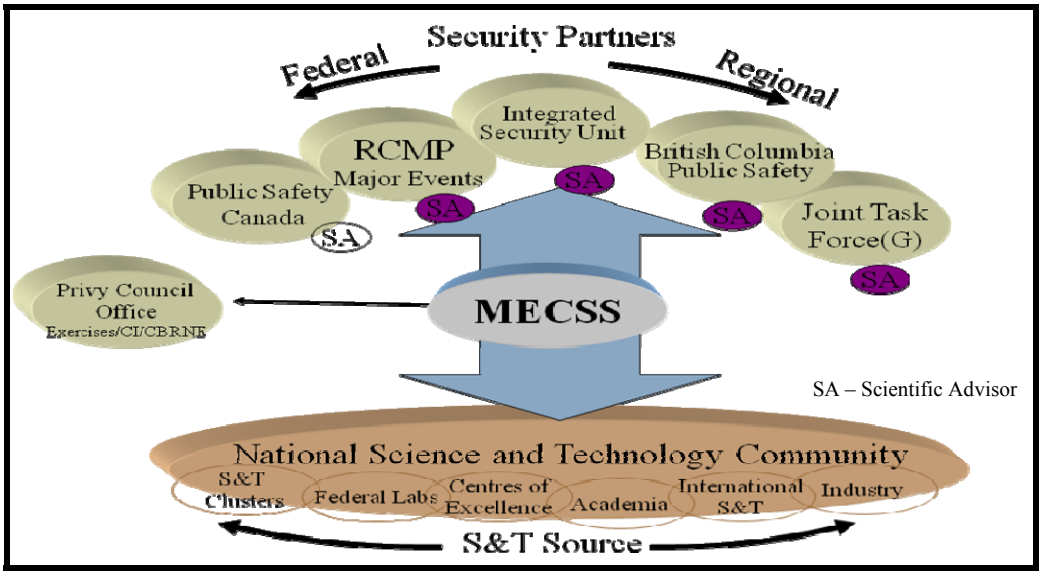

Figure 2: MECSS Delivery Model

1.3 Achievements

The MECSS Project successfully contributed to the reduction of security risk associated with V2010 and the G8/20 through the coordinated application of science and technology to deliver timely and operationally relevant advice. It achieved this primary objective within the resources assigned. This section will consider achievements within the context of Pre-deployment, Deployment and Legacy.

1.3.1 Pre-deployment

Within the Pre-deployment Phase, achievement can be measured by the degree to which S&T advice and support was delivered at critical junctures in the development of security plans with deliverables that were incorporated into V2010. The MECSS project produced a large number of scientific reports for the security partners, which reflects the degree of S&T uptake that had a direct impact on the security planning processes and the subsequent plans. For example, the ISU Physical Security plans pertaining to pedestrian/vehicle screening used scientific research and analysis as the foundation for much of their planning. The CBRNE posture achieved by the Province of BC, as well as the associated plans and concepts of operations, reflect the S&T support developed in the years and months leading up to V2010. Similar examples exist within each of the other primary MECSS domains including Command and Control, Surveillance, Critical Infrastructure, CBRNE and exercises. The following paragraphs offer a short summary of achievements in these domains.

Within Command and Control (C2), S&T contributed to significant enhancements of the Communications Information Systems (CIS) posture for the Canadian Forces. This included implementation of a portal for information sharing, a web application automating situational awareness of the C2 status during the operations, and improvements to Command View that is the primary tool used by the CF for situational awareness. DRDC also contributed the Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) mobile laboratory from DRDC Valcartier, which provided the CF with a mobile Level 3 C2 capability.

Within the Surveillance domain, S&T provided a spectrum of operational analysis in both the air and marine domains, to support planning. This included the options analysis of capabilities on which deployment decisions were based - in particular, marine force protection considerations in the vicinity of the Athlete's Village. The Automatic Ship Imagery system camera is another example of equipment that was deployed in support of the CF.

S&T support to Critical Infrastructure (CI) had a profound impact on the planning and operational posture of the ISU and the Province of BC Integrated Public Safety. This included the modeling of the CI interdependencies associated with the venues. Support also included blast modeling as a decision support tool.

MECSS was able to leverage the deep expertise within the federal S&T community and facilitate a significant degree of support in the domain of CBRNE. This included the coordination of the planning associated with Science Town in support of the RCMP National Team. S&T also supported the development of capabilities within the Province of BC, through close collaboration with Emergency Management British Columbia (EMBC). Support was also provided to municipalities, where appropriate. Much of the S&T provided was an extension of ongoing work provided through the CBRNE Research and Technical Initiative (CRTI).

The Pre-deployment Phase also included a significant degree of support to the series of exercises leading up to V2010. This included localized tactical level exercises, up to and including the national Exercises: Bronze, Silver, and Gold. Exercise designers used scientific expertise to guide scenario development, while the exercise leadership used the output of scientific analysis to assess the success of the Exercises, and to modify plans and protocols in preparation for the next

Exercise, or for V2010. This work involved a significant number of scientists from across the DRDC Centres, and played a large role in earning the respect of the security delivery teams. This was a significant accomplishment for MECSS.

1.3.2 Deployment

During the Deployment Phase, there were a number of S&T elements postured to support the primary security delivery organizations. Within the authority assigned to DRDC through the V2010 Deputy Minister's Security Advisory Committee (DM SAC), the MECSS Project led the coordination of federal departments in the deployment of Chemical, Biological, and Radiological laboratories to support the RCMP National CBRNE Response Team at both Olympic sites: Vancouver and Whistler. This capability delivered timely S&T expertise beginning several weeks prior to V2010 and throughout the security operations of the Olympics. This deployment validated the 'Science Town' concept and earned the confidence of the Public Security community as illustrated by the request for Science Town to deploy in support of the G8 and G20 Summits.

The Deployment phase also included an S&T reach back network which delivered expert advice from within a 24/7 posture. This network included Scientific Advisors at each of the primary Operations Centres within the Integrated Security Unit, Emergency Management BC, and the Government of Canada Operations Centre, who had contact access to expertise through centralized reach back coordination within the Centre for Security Science. As well, ADM (S&T) was included in the network where he sat on the Assistant Deputy Minister Emergency Management Committee (ADM EMC), which met daily throughout V2010. Reach-back requests were made on several occasions throughout the security operations, offering advice and information to leadership within the Ops Centres. The embedded scientific advisors were used in a consultation role within several of the Centres where support was provided. Again, this was a significant accomplishment for the science community, and was called on again for the G8 and G20 Summits.

During the Deployment Phase, DRDC also deployed Scientific Advisors in response to the ISU and CF requests for specific expertise, available on a 24/7 posture for the period of V2010. This included direct support to the ISU Physical Security Team, as well as the Critical Infrastructure response cell. It also included the deployment of expertise and kit in support of the CF and Joint Task Force Games (JTFG).

The deployment of capabilities in support of an operation was a significant achievement for DRDC from the perspective of command and control, as well as logistics. A domestic operational deployment of this magnitude is non-traditional for DRDC, and required careful consideration on how people would be deployed and employed within the C2 structure of other agencies and departments. A command and control relationship was established with those agencies that DRDC scientists would be responsive to during the operations. In the case of Science Town, a letter of agreement was setup between DRDC and the RCMP National CBRNE Response Team, and a C2 hierarchy was promulgated in the Ops Directive – DRDC Support to V2010. During the deployment, an operational rhythm was established including daily briefs to ADM(S&T), to ensure he maintained effective oversight of DRDC ops, and to ensure he was prepared to fulfill his responsibilities as a member of the ADM Emergency Management Committee. As well, this deployment was a catalyst for the drafting of the DRDC Human

Resource Policy on Domestic Deployments, which satisfied many of the logistical challenges, including compliance within the scope of collective agreements. The establishment of a posture within DRDC to support domestic operations was a significant accomplishment for MECSS.

1.3.3 Legacy

MECSS has delivered a solid list of legacy outcomes. First, a significant contribution to the legacy outcomes is the approximately 195 scientific reports that have been developed in support of security operations associated with Major Events. As well, the Major Events Framework builds an integrated planning methodology into the RCMP planning process; therefore allowing for a 'whole-of-government' approach to future planning of Major Events in Canada. A long-term relationship has been established between the Centre for Security Science and the RCMP Major Events Section by the placement of a Scientific Adviser into the RCMP spaces. The project has also created the conditions for many more legacy outcomes. Certainly, through MECSS, certain elements of S&T expertise and capabilities have been operationalized, allowing for greater resilience within the public security community, and posturing for greater support in the future. The S&T network put in place for V2010 received high acclaim from the leadership of certain Operational Centres, and is now seen as a standard for delivering S&T support within an operational context. There are many other legacy outcomes associated with MECSS, which are not easily measured. For example, the relationship between the S&T community and the Province of BC Emergency Management has been highly productive, and may be used in the future to advance operational capabilities, supported by S&T.

1.3.4 Conclusion

The MECSS project represents several significant achievements within the Science and Technology community. Within the scope of the identified resources, MECSS successfully assisted the functional authorities in reducing the security risk associated with V2010, through the coordinated application of science and technology. The Project outputs and deliverables successfully enhanced the confidence of the Public Security operational domain to employ S&T within the context of risk mitigation, trusted advice, knowledge generation and innovation.

Overall, the greatest achievement and outcomes of MECSS were a consequence of the day-to-day work of those scientists who interacted within the security teams. This work earned the scientific community the integrity and trust that created an ever-increasing number of opportunities for S&T to demonstrate value-added. Although the project delivered many tangible outcomes, as witnessed through the approximately one hundred and eighty five scientific reports, a large measure of the project's achievements are buried in non-tangible outcomes, which are not directly apparent and therefore difficult to measure. An example is the degree to which the exploitation of S&T evolved from "being offered" to "being asked for". This shift reflects a significant advancement in the maturity of the relationship between S&T and the operational community within public security. This is considered a significant achievement for MECSS.

2 Technical Performance

2.1 Scientific Advisor Joint Task Force Games

The role assigned the Scientific Advisor (SA) JTFG was the same as assigned to the other MECSS SAs but it had to be executed in a very different manner. The JTFP/MARPAC ORT Team Leader was formally assigned the role of SA JTFG at the start of MECSS but the major aspects of the position had already been part of the JTFG planning directive drafts during the summer of 2007. The direct linkage to a military sponsor simplified the integration of the SA JTFG into the JTFG planning staff because most of the senior staff had previously worked with DRDC.

The JTFG staff focus on meeting a tight schedule meant they were inclined to focus on obvious options. The SA challenge was to look for strategic points where DRDC capabilities could be leveraged to support what JTFG identified as their most pressing needs. The SA then had to quickly orchestrate reach-back with MECSS while negotiating expectations with JTFG senior staff. The most important skills were a sense of timing and ability to package options in a way the operators could appreciate.

The SA working relationship with JTFG staff was heavily influenced by:

a. JTFG started with a small cadre of officers focused mainly on applying the Operational Planning Process (OPP) to compile the required enabling documents;

b. JTFG needed help with how to integrate its C2 processes with the ISU well before the JTFG C2 structure jelled in early 2009; and

c. The majority of the JTFG staff with Land Force backgrounds had very little direct experience working with DRDC except as part of equipment experiments.

A timeline of the full body of work makes for an impressive diagram with a wide range of major projects. The activity included coordinating 3 significant initial projects, leading 8 distinct command and control activities, helping to facilitate 7 maritime activities, and leading/working on the analysis support to 11 exercises. The project complexity was substantial because many were concurrent activities that forced juggling within and between several disparate tasks. The SA activities were clustered into four distinct phases starting August 2007 until MECSS ended in May 2010:

a. Phase 1 from August 2007 to March 2008 started with the SA JTFG acting as DRDC POC at the ISU to identify S&T issues and tackle those with implications for DND. Work also included the initiation and coordination of several MECSS activities;

b. Phase 2 from April 2008 to August 2008 was the detailed C2 architecture analysis advice during the preparation of the ISU C2 CONOPS while transitioning the DRDC POC to the SA ISU;

c. Phase 3 from September 2008 to January 2010 was analysis support to the ISU and JTFG during major C2 training exercises, and

d. Phase 4 from February 2010 to May 2010 was the deployment as SA to the actual V2010 Games and preparation of project documents.

There were many points during V2010 where DRDC actions had a clear, decisive and enduring impact on how JTFG evolved and learned to conduct business. Some examples of DRDC activities for JTFG included:

a. JCDS21 Experiment 1 created exercise content and used DRDC assets to give JTFG staff an early opportunity to work as a command team in proximity with the ISU at Pegasus Guardian in November 07;

b. Initial Vehicle Screening Aarea (VSA) analysis in February 2008 quantified resource needs and risks involved if the CF decided to provide VSA screening teams;

c. Games Red Teaming (GRT) concept was fostered within the JTFG planning process. MECSS funded a Military Reservist and provided access to DRDC Red Teaming expertise;

d. Conducted a comprehensive analysis of V2010 C2 Architecture;

e. Conducted a comprehensive analysis of ISU and CF Games Joint Operations Centres (GJOC) layouts;

f. Used JCDS21 Experiment 2 to expose JTFG operators to the latest CIS technology;

g. Rapid deployment of JCDS21 assets to mimic the necessary JTFG C2 structure in Exercise PG 2 (during ISU Exercise BRONZE);

h. Analyzed multiple exercise events with turnaround of reports within days;

i. Integrated DRDC and JTFG assessments of a new Diver Detection system;

j. Deployment of Automated Ship Image Acquisitions (ASIA) camera to monitor a strategic waterway narrows; and

k. JTFG Information Technology Architecture documentation and gap analysis while JTFG deployed.

In retrospect, the workload of the Scientific Advisor JTFG would have justified making it a dedicated position instead of assigning it on top of similar duties for another operational headquarters (JTFP). In the future, the SA should be co-located in the same building as the military partner to ease collaboration and should be added to the JTFG organizational chart to show clear lines of responsibility and accountability.

2.2 Scientific Advisor V2010 Integrated Security Unit

The SA ISU was located at the Integrated Security Unit (ISU) in Richmond, BC and was deployed from early July 2008 through to 31 March, 2010.

The primary client was the ISU. A secondary client, as time went on and ISU support requirements diminished, was Integrated Public Safety (IPS). Within the ISU the primary client was the RCMP but since the ISU had representatives from various organisations, they became clients when circumstances warranted such as Transport Canada and the Canadian Forces. In most cases, a task would support a group of clients that included representatives from several organisations.

In the early days after deployment, the priority was to begin to establish the connections with the various possible stakeholders at the ISU and also to become familiar with both the ongoing DRDC projects and also with the evolving needs of the ISU. Because of the foundational work by Ron Funk in particular, these tasks were much easier as there were clear starting points.

In general, the approach was to talk to the people at the ISU and learn what their job was and what their problems and challenges were. In addition, an understanding of how the ISU itself functioned was necessary and was developed. The awareness of the people and processes translated into becoming aware of various meetings where the key issues were discussed. Getting to know the people and attend their meetings was the key to getting the overall understanding of many of the streams of activity at the ISU and therefore where DRDC might best be able to contribute.

This process of meeting people and establishing connections was ongoing throughout the deployment period but the focus of the networking changed as DRDC's capacity to support new tasks was reached. The SA ISU focussed on facilitating the defined tasks, contributing to them directly when feasible but at the same time continuing to stay abreast of ISU activities in case support from DRDC was needed somewhere new. MECSS took on additional tasks through 2009 as other support activity wound down and capacity became available. This was the approach followed for the duration of the deployment.

In general, there was not a problem with having to choose one project (support request) over another. The number of projects that the SA thought required support were relatively small and within the capacity of MECSS to support. In all cases, the projects that MECSS supported were judged to be very important for the success of the Games security. The SA applied his broad knowledge of the scientific capabilities within DRDC to recognize which ISU activities could benefit from DRDC assistance. Deliverables and delivery timelines were also considered when considering a possible support activity. It turned out to always be obvious that DRDC had the capability to provide support – it just became an issue of capacity based on the available resources.

The original intent was that the SA ISU would directly advise the Chief Operating Officer (COO) at the ISU on S&T matters. This arrangement never materialised and instead, the senior level contact became the Canadian Forces Liaison Officer (CF LO) at the direction of the V2010 ISU COO. This meant that the SA had no significant contact with the COO or the Operations Officers for the duration of the project. The result was that the value of S&T to these key decision makers

had to be pushed from "the bottom up" and through several levels on the organization chart. The relationship with the CF LO was very good and he was a very strong supporter of the application of S&T in support of operations. He was always an astute observer of the political situation within the ISU which helped the SA navigate the client sensitivities.

The SA focussed support work at the "tactical" level, allowing the RCMP/ISU client to get authorisation for DRDC support through their chain of command. This also meant trying to get "pull" from the ISU in response to offers for S&T support. This was accomplished by first identifying a support area that DRDC was qualified for and then discussing how DRDC might be able to contribute. The request was often done informally (verbally) but in cases where substantial resources would be needed (like for exercises), the client was asked to provide a written request. The ISU clients had limited experience with DRDC or S&T support and therefore they were unaware of the kinds of things the federal S&T community could provide. Despite this, they were highly supportive of the work undertaken and saw the value of the outcomes. From Day 1 of MECSS, we had to be careful not to oversell what we could support and how fast we could provide results. Managing expectations was something that had to be done throughout the project.

Because of the liaison and coordination role, the SA facilitated and/or contributed to every task that DRDC supported for the ISU. In some cases, the involvement was direct in that the SA collected data, led a team and/or contributed to reports. This was particularly true of the exercises from BRONZE on, the VSA exercises and the CONAF work.

The tasks where the SA's contribution was more direct included the following:

a. C2 System Hardware Requirements. The ISU SA worked with Subject Matter Experts (SME) from the Communications Security Establishment (CSE), the CF and the RCMP to provide the ISU with an assessment of the two options for building the ISU's C2 network.

b. Confirmation Architecture Framework (CONAF). A modified DND Architecture Framework was proposed to the ISU and IPS exercise planners in April 2009 as a method for defining metrics that could be used for confirming the readiness of the ISU for V2010. It was mostly useful as a planning aid and gave each group a much clearer picture of their business, the processes they needed and who they needed to liaise with.

c. Crowd Flow/Behaviour Analysis. This was an exploratory activity only. The intent was to provide the ISU venue planners with a way to assess their venue layouts for any safety implications if a crowd evacuation had to be performed and also to allow for some assessment of traffic and crowd flow in the streets related to spectator movement to/from venues.

d. Exercise Support. The SA ISU was the lead for all S&T support to the ISU Exercise Program. The range of activities covered support to and leading of analysis teams, developing analysis/assessment plans, facilitating table top exercises (TTX) and applying the CONAF methodology.

e. Vehicle Barriers. A reach-back request in May 2008 from the Physical Security Unit asked about DRDC/CF data on vehicle barrier stopping power and approved devices. A response was provided shortly after which satisfied the request.

f. Vehicle Screening Areas(VSA)/Pedestrian Screening Areas(PSA)/Remote Vehicle Screening Sites (RVSS). Several field trials were run to support the development and testing of designs for the VSAs and PSAs. The SA was engaged in both data collection and leading of portions of the Exercise Blue VSA trial.

Enablers of/Challenges to Mission Success

a. MECSS Project. Provided the mechanism to link the ISU with S&T. Had strong support from senior DRDC management and a budget large enough to permit the flexibility to engage in a variety of tasks. The SA ISU was able to operate with autonomy and flexibility which worked very well for establishing working relationships, identifying key issues and being able to adjust as necessary to the changing environment at the ISU.

b. Working relationships. Relationships with our clients were a key enabler in delivering S&T within the V2010 ISU. Planners were appreciative of our S&T expertise and eagerly embraced the support we provided.

c. DRDC Culture. DRDC personnel who came out to BC were professional, motivated, creative, supportive and mission-focused.

Key Challenges

a. The new working relationship between DRDC and the RCMP ISU created a number of challenges as each group came to understand the requirements, methods, and build and environment of trust.

b. DRDC was not used to responding to reach back requests on very short (days or a week) timelines. In most cases, a response was obtained rapidly enough but in some cases, delivery deadlines were missed. This had an impact on the quality of support that the SA could deliver to the ISU team.

c. DRDC Support to Deployed Staff. Support to deployed personnel within the context of a domestic operation was new to DRDC. This created significant distractions for the deployed staff in terms of logistics support. The centralized nature of MECSS sometimes challenged the SA's ability to execute activity based on his best judgement. The centralized control of overtime is an example of this. As well, the interpretation of departmental policy was sometimes a source of conflict, in an effort to resolve personal administrative issues. The distance also created challenges pertaining to IT support, which degraded the SA's capacity to deliver effect S&T support to the client. It is the assessment of the SA ISU that the MECSS team should have had greater administrative and IT support to better accommodate the needs of the deployed staff.

2.3 Scientific Advisor Integrated Public Safety

The SA visited the Integrated Public Safety team (IPS) at the beginning of August 2008 upon commencement of the assignment and was located full time with the IPS group (within the ISU building) in Richmond, BC from September 2008 to mid-April 2010. The primary client was the Province of BC IPS. As well support was provided to the South West Provincial Regional Emergency Operations Centre (PREOC), the City of Vancouver (CoV), and the ISU.

Overall Observations

a. DRDC could have done better in supporting staff on long-term domestic travel status to areas without DRDC facilities. Support for relocating, clarifying travel directive issues, and resolving technical issues in a timely manner could be improved. The resolution of issues was time-consuming and, on occasion, stressful, and distracted from the activities of the position.

b. Relationships with the clients and trust are of utmost importance. SAs need to be integrated in teams on-site so that they can interact with clients regularly to build relationships and trust, have awareness and understanding of issues as they arise, and be able to seize opportunities.

c. The degree to which S&T was embraced was heavily dependent on the person in charge of a given domain and others who had influence. Ideally, each project task needs support from all levels. As witnessed through several tasks, one "non-supporter" in a critical position can stall or stop progress. It would have been beneficial to have the SA integrated with the team on the ground earlier, to have been involved full-time in several critical DRDC activities (such as Critical Infrastructure) from the beginning.

C2 Analysis Support for the PREOC

C2 analysis support was engaged to assess and enhance the PREOC's state of preparedness for V2010 and to provide feedback on operations during the Olympics and Paralympics. This included:

a. Operations analysis during Exercises Silver and Gold as well as during the Olympics and Paralympics. The observations and recommendations provided led to significant changes in operations for the Olympics and Paralympics and identified areas requiring further attention.

b. Extensive work by the IPS and ISU SAs and EMBC staff between April 2009 and Exercise Gold as part of the "CONAF" effort, with the application of architecture frameworks to the PREOC. The CONAF work led the PREOC to the realization that they needed to develop a Concept of Operations document for Games time, which became their primary reference document for operations.

SA During Olympics/Paralympics.

The SA IPS was engaged in the operations centre (PREOC) during Games time (in the Planning Section as Scientific Advisor), with the SA RCMP providing backup support. The role of the SA was to provide scientific advice in areas of expertise (for example, supporting the CI Unit and linking to the key cyber stakeholders), liaise with Science Town for CBRNE-related scientific/technical questions, provide a reach back capability to DRDC subject matter experts (SMEs), and use connections into the broader science and technology community as required. Through the establishment of trusted relationships with the PREOC staff, DRDC was given an active role in emergency management operations and was poised to immediately bring S&T expertise to bear where appropriate.

Critical Infrastructure (CI)

The IPS SA supported the CI activities, with the exception of the blast analysis, and led the IPS CI outreach to asset owners at the request of Manager IPS. At the start of the assignment, the former Director IPS had asked the SA to focus on providing CI support to IPS and the Joint Emergency Liaison Committee (JELC) CI Working Group. However, upon arrival in BC, the DRDC criticality analysis for the ISU was well under way and events to that point had influenced attitudes towards DRDC. The gap between the security and safety partners proved challenging in providing effective support. Through the CI work, a very strong relationship was developed with the ISU CF LO. This relationship proved to be invaluable as the LO was DRDC's biggest champion on the ground. Being involved in the CI analysis work from the start would have been beneficial in influencing program direction.

CBRNE

The IPS SA was a member of the Provincial CBRNE Working Group. Involvement in this group was instrumental in getting DRDC involved with the BC CBRNE capability and gap analysis. This task paved the way for much of the DRDC work that followed with BC leading up to V2010.

Cyber

The IPS SA initiated and participated in a cyber task – for more information see the Cyber section of the report.

2.4 Scientific Advisor Royal Canadian Mounted Police

The role of Scientific Advisor to Major Events and Protective Policing Services (ME&PS) became operational in April 09. The primary role was to support the RCMP through MECSS providing analytical support and scientific advice with the secondary role to develop the Major Events Security Framework (MESF).

The SA to RCMP was engaged in a broad variety of activities. As a fully engaged member of ME&PS, the SA was included in the regular briefings and engaged directly with staff to develop the MESF. As well, the SA was engaged as an analyst to support the RCMP during the Olympic exercise program.

From 28 September to 6 October 2009, the SA attended the National Operations Center (NOC) Incident Director All-hazards Course. The NOC Incident Director course is designed to increase the knowledge and develop the skills of members who will be called upon to act as Incident directors in the NOC. The course provides comprehensive learning activities that address all-hazard types of events as well as exercises in preparation for V2010 and other upcoming major events. As part of the course the SA was asked to evaluate the TTX for the NOC. Additional analytical support was provided by DRDC Valcartier and CSS.

The NOC TTX was orchestrated as a forum to evaluate current information interoperability plans, concepts, resources, and interoperable capabilities. From an analysis perspective, the TTX was viewed with a focus on interoperable information capabilities or gaps; interoperable information assets in place, or their absence; and the use of processes that support interoperable communications. A Letter Report was provided to the NOC upon completion of the TTX.

Exercise Pegasus Guardian III (PG3) was the fourth and final command post exercise in the Pegasus Guardian series designed to test the security preparations for V2010. The SA was assigned to provide analytical support to the Vancouver Area Command Centre.

The aim of EX Gold was to confirm a functional, integrated command and coordination structure with effective information and intelligence sharing in support of the Canadian national security and emergency management framework for the 2010 Winter Olympic Games. The SA conducted analysis focused on information processes and protocols within and at the seams of the NOC. A Letter Report was provided to the NOC upon completion of the Exercise GOLD. One of the shortcomings observed revolved around the issue of Handovers. Leveraging the work of DRDC Toronto on Handovers and additional research into the problem space, a handover process was developed for the NOC in collaboration with RCMP Exercise Director.

In support of the 2010 Vancouver Olympic Games, the SA was deployed to Vancouver to act in the capacity of SA to the PREOC in addition to contributing to the Command and Control analysis. Following this period 1-4 March, lessons learned were gathered and subsequently compiled with regards to the deployment of science town. This culminated in the publishing of a letter report that will inform future deployments of S&T support.

Development of the MESF had the full support of the ME&PS leadership and was actively supported by the RCMP staff assigned to the task. The development progressed along four main themes: creating the foundation; identifying technical solutions; capturing the planning process; and building the solution. During the course of its development over 40 workshops were facilitated in order to design the operational vision and content for the MESF. It has been decided that the MESF will become a legacy element of MECSS, and follow-on activity will occur post-MECSS as a separate activity under PSTP.

2.5 CBRNE Domain Lead

CBRNE S&T was prominent in the planning and operations associated with V2010 as well as the G8 and G20. This was true at each of the federal, provincial, and municipal levels. The nature and complexity of the issues associated with CBRNE required a strong degree of expertise from across various Agencies and Departments. The capabilities and experience stemming from

investments made through CRTI played a prominent role in the degree to which the security partners were able to plan, prepare and exercise for a CBRNE event.

From October 2008, the CRTI CBRNE multi-agency community of expertise began working with PCO, Public Safety Canada (PS), the Canadian Forces (CF) and the province of BC. Outcomes of this activity included the development of a Federal CBRNE Capability Inventory, Federal CBRNE CONOPS, Federal CBRNE Protection Plan for V2010, CBRNE Capability and Gap Analysis for the Province of BC, and a BC CBRNE Consequence Management Plan. The CBRNE domain, with contractor support, also conducted CBRNE Sensor Placement Studies and served in an advisory capacity to PS and Canada Command in the development of their V2010 CBRNE Plans. This included liaison with the US leading to the development of a Concept of Operations in support of Canada/US Civil Assistance Plan activities. Further to this and in recognition of gaps that existed at the provincial and municipal level, MECSS coordinated the provision of equipment and specialized training to create multiple teams within the greater Vancouver area capable of working in a CBRNE environment.

MECSS delivered the following:

a. Federal CBRNE Capability Inventory: This work served as the foundation of the PCO-led Federal CBRNE Protection Plan.

b. BC CBRNE Capability and Gap Analysis: This work was conducted at the request of the Province of BC. Through relationships established under CRTI Exercise INITIAL THUNDER, Emergency Management BC progressively sought the support of DRDC in their understanding and development of CBRNE capabilities. This work served as the foundation for decisions pertaining to the BC CBRNE Consequence Management Plan

c. CF CBRNE Sensor Placement Study: The CF was tasked with force protection of a portion of critical infrastructure in downtown Vancouver. As part of their plan, they requested DRDC support in determining the most efficient location for a series of CBRNE sensors to accommodate a suitable level of protection. The study was delivered to the CF; however, the conditions that would require the placement of the sensors did not materialize.

d. CBRNE Training: As follow-on to the type of investment made through CRTI, MECSS was able to support the delivery of training to a number of provincial and municipal organizations within the lower mainland of BC. This included Vancouver City Police, local health care organizations, and others including a workshop for the BC Office of the Coroner.

e. CBRNE Tabletop (TTX) and Live Play during Ex Gold: Leveraging the CRTI investments, MECSS was able to design, develop and deliver a whole-of-government CBRNE TTX and the live play components of Ex GOLD. Overall, the S&T support to Exercises, including GOLD was significant.

f. Science Towns: Based on the investment of CRTI, MECSS was able to leverage on existing relationships and capabilities to develop the basic concept of operations,

command and control relationships, as well as coordinate the planning and setup of Science Town at each of the two primary Olympic sites: Whistler and Vancouver. Science Town is a multi-agency capability that brings together world class equipment and expertise in support of the RCMP National CBRNE Response Team.

In addition, MECSS contributed to the following:

a. Federal CBRNE CONOPS

b. Federal CBRNE Protection Plan for V2010

c. BC CBRNE Consequence Management Plan

An important outcome of this effort was the creation of Science Town. The origins of Science Town date back to the very beginning of CRTI. At that time, the focus of the program was on building capacity within Canada's laboratory structure to enable S&T work in the area of CBRNE counter-terrorism. The very nature and urgency of the problem meant that a great deal of weight had to be dedicated to developing and delivering the "tools" needed to combat risks posed to Canada by the CBRNE terrorist element. While that remains an important goal, it became apparent over time that intellectual capital had to be brought to bear in developing methods and protocols by which these new tools could be employed in an operational environment. The result of this thinking was that the initial CRTI emphasis changed from one of building "capacity" to one of building "capability".

Science Town represents the operationalization of national S&T capabilities, in support of the RCMP National CBRNE Response Team (N CBRNE RT). Through a detailed planning process, a series of exercises, and the provision of specialized training, the concept of Science Town was matured and first trialed at the 2008 Francophonie Summit in Quebec City. This led to follow-on studies and as well as the development of a 'first generation' concept of operations and standard operating procedures. In December of 2008, the RCMP N CBRNE RT formally requested S&T support, which was endorsed by the Deputy Minister Security Advisory Committee on V2010. Plans were then initiated to establish a cluster of mobile laboratories and associated expertise to be located in both Vancouver and Whistler. Senior CBRNE Scientific Advisors and mobile laboratory facilities were positioned in both locations to support critical incident response and consequence management activities that spanned the: prevent, prepare, respond and recover continuum of operations.

The CBRNE domain also played significantly within the national V2010 Exercise Program. MECSS coordinated the support of S&T expertise in the scenario development for Bronze and Silver as well as leadership in the design, development and execution of the live-play components of Ex Gold. During the final confirmation for V2010 (Ex GOLD), CBRNE events drove many of the key exercise scenarios.

Concurrent with much of the V2010 activity, MECSS was also engaged in the planning for S&T CBRNE support to the G8 and G20. This included the deployment of Science Town to both Huntsville and Toronto.

Given the strong background in CRTI, the CBRNE S&T community demonstrated a truly world class capability in support of national planning, exercises and operations. Science Town, for example, caught the attention of senior national leadership as well as visiting security officials from other countries, and played a significant role in mitigating the risk associated with CBRNE events during V2010, as well as the G8 and G20. This effort contributed to a more coherent approach to CBRNE counter-terrorism preparation, prevention, response and recovery planning in Canada.

2.6 Command and Control Domain

Notwithstanding the importance of communications and information technologies, Command and Control is fundamentally a human activity. Organization and technology exist to support the human dimension of decision-making. In essence, the C2 of major events can be viewed as systemic execution of collective collection and analysis of information, planning, decision-making, coordination, and sustainment of operations and activities. The Vancouver 2010 operations are multi-layered. V2010 C2 arrangements span across at least three pillars, each involving a set of heterogeneous and multi-jurisdictional agencies and organizations as shown in Figure 3.

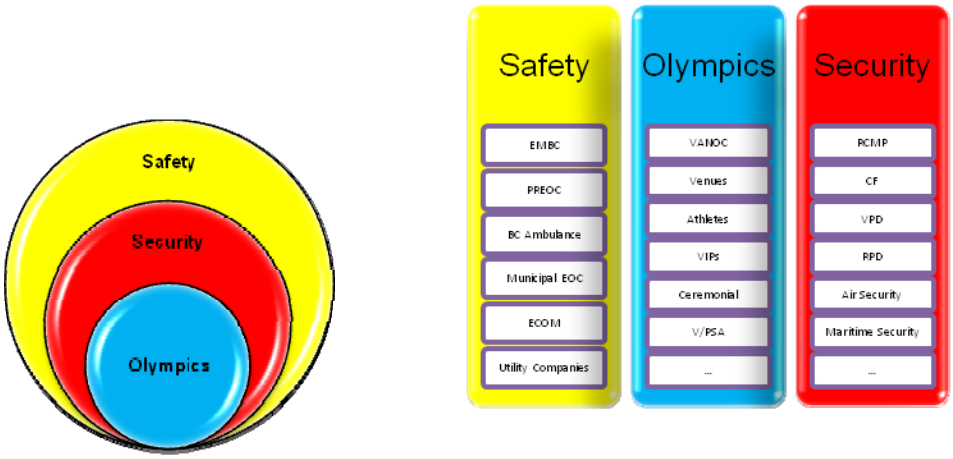

Figure 3: (A) Multi-Layered Operations: (B) Three Pillars with Multi-Stakeholders

Therefore, it is not surprising that the C2 has been the main integration layer for Vancouver 2010 operations. Vancouver 2010 C2 involved many organizations and Command and Operations centers scattered throughout the Vancouver and Whistler. Moreover, many other centers have been integrated in this C2 concept of operations. Coordination and integration of many agencies and stakeholders involved huge enterprise coordination and management effort. Key coordination effort includes determining objectives, establishing the appropriate competence, authority and responsibility constructs, and allocating resources. Direction has become synonymous with Common Intent. Cohesion and inclusion of different agencies and stakeholders have become important enablers and unified direction for success. Therefore, Command and Control of major

events is a very dynamic domain. Communication, coordination, collaboration and integration have been considered key enablers for a successful C2 solution. Shared situation awareness, common intent, trust in distributed teams, communication and information strategies are key foundations for major events C2 effectiveness. Consequently, maintaining a common knowledge base and sustaining trust among heterogeneous stakeholders and organizations has been the main C2 challenge during Vancouver 2010.

MECSS C2 team has been involved with the following activities in support of V2010 C2:

a. Command Centre Design: This activity involved science and technology (S&T) support for performing ergonomic analysis and workspace design for ISU operations and command centres. A series of studies have been conducted in which workspace solutions were produced for Theatre Command Centre, Vancouver Area Command Centre, Whistler Area Command Centre, Air Support Operations Command Centre, Olympic Marine Operations Centre and CF Games Joint Operations Centre. In these studies, a new design process, Alternative method for Workspace Analysis and Design (AWAND), was proposed and then further developed.

b. IT Architecture Options Analysis: This work involved consulting with a number of experts in network design and providing some input on the impact of selecting a thin versus thick client network architecture for the ISU.

c. JCDS 21 EXP 2 at Star Top: MECSS leveraged JCDS 21 EXP 2 in order to offer an opportunity to GJOC for training and testing the C2 CONOPs. Following that event, JTFG requested that JCDS 21 test bed be deployed to Richmond to provide GJOC CIS infrastructure for EX BRONZE. Most of JCDS 21 equipment was provided to JTFG for their use. MECSS also coordinated a multi agency C2 demonstration day that engaged nine (9) C2 solutions and two (2) mobile Command Posts.

d. CIS Study for JTFG: MECSS conducted a survey of recent operational C3IS deployments within Canada and abroad in order to provide advice for JTFG V2010 CIS planning. This work focused on:

   - C2 process and applications deployment and support issues and their adequacy to the Commander and war fighter requirements,
   - information Protection and security issues and vulnerabilities and mitigation processes,
   - information exchange challenges with other agencies and information flow issues between the different level of command,
   - infrastructure design, implementation and sustainment,
   - Crypto support (tactical thru Strategic),
   - user-Helpdesk-Consolidated Support Desk integration, synchronization and harmonization, and
   - operational plenary, prioritization, command, coordination, consultation processes and interagency integration protocols.

e. ISU C2 CONOPS: This activity contributed to the development of ISU C2 concept of operations (CONOPs) by conducting a quick set of stakeholder interviews, as well as the drafting of the initial narrative for the ISU C2 CONOPs. The deliverables have then been integrated into the final ISU C2 CONOPs.

f. V2010 C2 Architecture and Process Modeling: This activity provided analysis support to help the ISU and its security partners to build a viable C2 architecture. This work helped to identify functional goals, articulate the aligned operational processes and determine the IM/IT systems needed to support them. The work leveraged the knowledge gained from Exercise Pegasus Guardian and prior work modeling C2 Architecture for other segments of the CF.

g. Collaboration Framework: This work was done to support the ISU and exploited previous DRDC work in order to provide advice as to how the various organizations involved in domestic security during the 2010 Olympics might optimize their collaboration in order to maximize operational effectiveness. Moreover, MECSS leveraged the database of more than 400 questions to evaluate collaboration during different V2010 Exercises.

h. Confirmation Architecture Framework (CONAF Work): CONAF work was initiated to support V2010 ISU C2 confirmation, by providing functional groups with a framework for developing a set of criteria that could be used during the final exercises (PG3, GOLD, TTXs) to confirm their state of readiness/preparedness for V2010. The CONAF structure articulated what the process is, how it relates to the business and who needs to be a part of the process. The discussions also facilitated bringing together groups who had never met to talk about processes linking them.

i. Deployment of DRDC C4ISR Mobile Lab: Following EX PG2 (EX Bronze), the DRDC C4ISR mobile lab was transferred to JTFG for deployment in support of Vancouver 2010. The work under this activity provided S&T support to JTFG in order to upgrade, employ and redeploy the C4ISR Lab as a mobile Communication and C2 capability.

j. OMOC Analysis: The work under this activity provided operational analysis support to the OMOC, primarily through the application of a methodology for conducting a table top exercise, known as the Australian Force Protection Matrix Game. The delivery of three Matrix Games was well received by the OMOC planners and led to further requests for focused analytical support to OMOC during all major exercises and the execution of the Games.

k. Information Sharing Options Analysis: This activity was initiated in support of the JTFG to examine different IT options for information sharing and collaboration between different JTFG elements. A report presented different feasible options.

l. Shift Scheduling and Mobilization Planning: This activity was initiated to develop optimization model and application for work force scheduling employees at various distinct locations. The proposed model took into account the varying staffing levels required throughout each day at each location. As well it was flexible enough to

allow for changes in the staffing levels, and assists in planning in cases of surge requirements. The model could also create. Late changes in the ISU CONOPS for personnel deployment precluded the use of the output of this application.

m. Support to JTFG J6: Throughout the planning and execution of operations in support of Olympic security, MECSS provided dedicated scientific advice to the JTFG J6. This included options analysis, technical and scientific advice, system management and deployment.

n. Link 16 Analysis: This activity provided operational analysis during the CF component of Ex SILVER, to assess the Link 16 Network within the CF, including the Joint Interface Control Cell (JICC) operations. The result was a classified report.

o. CIS architecture, documentation and analysis: This activity involved the survey, documentation and analysis of the proposed CF CIS architecture across the Joint Area of Operation. A set of interactive documents were delivered to JTFG and deployed on Command Net to support planning, trouble shooting and redeployment of JTFG CIS infrastructure. These results were also used to provide the Commander of JTFG with an assessment of the CIS Operational Readiness.

p. Deployment of Information Sharing Solution on Command Net: MECSS implemented an information sharing and collaboration portal based on SharePoint, including a CIS dashboard used for daily commander's briefs. The SharePoint solution is an V2010 legacy that will be transitioned to JTFP or other Canada COM organizations.

q. Deployment of BattleView Software and Hardware: At the request of the JTFG LO at the ISU, an instance of BattleView was installed to accommodate a familiarization of the software application.

r. Information Request Manager (IR Manager): MECSS invested in creating a federated version of IR Manager with the intent of using it during V2010 to support reach back into the federal S&T community. Due to time constraints, the full utility of the tool was not employed during the Olympic security operations. IR Manager is legacy item for MECSS and will be implemented by Public Safety Canada and DRDC

2.7 Critical Infrastructure Domain

During March 2007, a group from DRDC that included representatives from the Centre for Operational Research and Aanalysis (CORA) and CSS as well as the DRDC R&D Liaison Officer to Canada Command met with the V2010 Integrated Security Unit to discuss areas on possible DRDC contributions or support. Several potential areas were identified. One potential area included "Critical Infrastructure Protection" and the "mapping out" of critical infrastructure (CI). DRDC's potential contribution was identified as the conduct of risk analysis on V2010 related infrastructure. In August 2007, the JTFG Operational Research advisor met with ISU staff. Again, a potential contribution for DRDC was identified as "vulnerability and risk assessments" including assessment of vulnerabilities due to CI dependencies. Once DRDC established the MECSS project, CSS Operational Research Team (CSS ORT) was requested by

the MECSS PD to provide early on-site OR support for the ISU until full-time Scientific Advisors (SA) were deployed. During the first on-site support visit by the CSS ORT the ISU and the provincial Integrated Public Safety organization requested support with respect to CI. Several CI related activities that were eventually carried out by the CSS ORT, the IPS SA and blast modeling experts from the Canadian Explosives Research Laboratory (CERL) and Martec Ltd.:

These items will each be discussed in turn.

a. 2010 Asset Criticality Analysis. The Chief Operating Officer (COO) of the ISU indicated that understanding the vulnerability of V2010 games and security operations to CI dependencies was a priority issue since there were suggestions that substantial security personnel could be required to ensure adequate security. Work was initiated in April 2008, an interim report was delivered in August of the same year and a final report was delivered in January 2009. A key factor affecting the delivery of the final report was that non-disclosure agreements (NDA) were not signed between the RCMP and asset owners until the fall of 2008. The immediate outcome of the 2010 Assets Criticality Analysis was to provide guidance to the ISU for directing the allocation of scarce resources in liaison meetings with the more critical asset owners. The eventual outcomes of this process were (1) the establishment of an effective information sharing process between the ISU and key asset owners and (2) confidence within the ISU that adequate preparations were being taken to reduce risk due to CI dependencies.

b. V2010 Venue Blast Vulnerability Analysis. A key concern of ISU planners was the potential risk due to the threat from intentional explosive attacks. Of particular importance for the ISU planners was the development of adequate security solutions for the venues in highly congested area of downtown Vancouver. While planning guidance for stand-off safety distances with respect to explosives is available from a variety of sources, this guidance has significant limitations in an urban environment due to the complex interactions between blast pressure waves and the urban topography. Through the CRTI cluster, the DRDC MECSS CI team was able to provide the ISU with:

   - First order analysis for a number of venues through expertise resident in the Canadian Explosives Research Laboratory (CERL) that is a part of Natural Resources Canada; and
   - Detailed analysis for the downtown Vancouver venues of BC Place and GM Place through Martec Ltd., which had developed a detailed model for assessing blast effects in an urban environment through the CRTI program.

   The outcome of this work was that it provided the ISU with valuable information for the development of appropriate security solutions and with appropriate knowledge for its negotiations with the City of Vancouver with respect to street closures.

c. UBC i2sim Research Project. Public Safety Canada and the National Science and Engineering Research Council (NSERC) of Canada had funded several research initiatives to better assess, manage and mitigate risks from the failure of CI due to interdependencies. At the time of the initiation of the MECSS project, the only

initiative that was sufficiently mature was the development of the i2sim CI interdependency simulation by University of British Columbia. This modeling capability was seen as having the potential to provide a valuable "what if" tool for planning, exercise and games time operations. When it became clear that the model would not be ready for ISU purposes, focus shifted to supporting the City of Vancouver emergency management and regional public safety. This latter solution encountered two problems which were (1) the lack of experience by provincial and regional planners with using simulation tools and (2) the lack of experience by the UBC team in understanding the operational community. While the i2sim work did not provide a direct benefit for V2010, it does provide a legacy value in providing DRDC with a CI interdependency modeling capability that can be used for future events. In addition, the lessons learned from the interactions between the UBC team and the local emergency management community, show:

- The need to assist local emergency management planners with the development of improved planning processes; and
- The value of scientific personnel, such as operational research scientists, having an in-depth understanding of the operational community in articulating their requirements for the scientific community and in explaining the benefits of S&T to the operational community.

d. Analysis of JELC Methodology. In support of the ISU, the provincial IPS employed a data collection and rating evaluation Excel spreadsheet developed through the Joint Emergency Liaison Committee (JELC) that had been established to improve coordination across CI sectors in the Lower Mainland region. DRDC provided feedback to IPS on the methodology.

e. Urban Domain Criticality Assessment. IPS Director requested that DRDC provide a similar criticality analysis for the IPS to what had been done for the ISU. The results were used for a follow-on outreach to key CI asset owners that collected valuable information that was made available to the Provincial Regional Emergency Operations Centre (PREOC) staff. Unfortunately, there was insufficient time prior to V2010 to provide support in interpreting the results.

f. CI Outreach to Asset Owners. Following the Urban Domain Criticality assessment the DRDC IPS SA used the results, in January 2010, to discuss CI issues with key asset owners that did not already have an established liaison link with the ISU. These discussions yielded information, which in the event of a significant CI disruption could have proven invaluable for PREOC and other regional response staff

2.8 Exercise Domain

Over the period of planning for the Vancouver Olympics, DRDC supported a number of exercises ranging from table tops to command post exercises to live exercises. This section of the closeout report gives an overview of the purpose and context of each exercise, what support was provided by DRDC and what the outputs and outcomes of that support were.

a. Privy Council Office (PCO) Exercises. The PCO (through the Office of the Coordinator for the 2010 Olympics and G8 Security) mandated that a series of exercises be conducted to support the "whole of government" approach to safety and security preparations for the Olympics. PCO setup a multi-agency steering committee which included MECSS for a representative of the S&T community. The Exercise series was composed of three complimentary exercises: BRONZE, SILVER and GOLD. BRONZE was intended as a mechanism "To Explore" the C2 relationships between the groups. SILVER was intended "To Practise" the established relationships and procedures and GOLD was planned as a way "To Confirm" the readiness of the safety and security structure.

   i. **Exercise BRONZE** (12-14 Nov 08) was a table top exercise with a regional focus. DRDC provided analysts to participate as controllers for the exercise as part of the Director Land Synthetic Environment (DLSE) assessment team. Other Subject Matter Experts (SMEs) were provided through MECSS to assist the discussion groups with technical expertise such as in CBRNE and psychosocial.

   ii. **Exercise SILVER** (9-13 Feb 09) was a command post exercise with some live play elements that continued to develop the C2 relationships within the safety and security pillars, expanding the exercise beyond the region to include Federal and international level stakeholders. DRDC supported the assessment for the Canada Command Joint Command Centre (JCC), the V2010 ISU and, for the first time, the Provincial Regional Emergency Operations Centre (PREOC). Within the ISU, analysts were present in the Theatre Command Centre (TCC) and the co-located Vancouver Area Command Centre (VACC). DRDC data collection methods involved in-situ observations and questionnaires. The reports were well received by Canada Command, the ISU and PREOC, serving to solidify requests for further support.

   iii. **Exercise GOLD** (2-6 Nov 09) was the final opportunity for the security and safety pillars to test and practise the C2 structure and procedures that had been developed and put in place. As at SILVER, DRDC provided assessment support teams to the TCC, VACC, PREOC and also to the Whistler Area Command Centre (WACC), NOC, GOC. Support methods involved in-situ observations and the administration of questionnaires and also included the use of the Confirmation Architecture Framework (CONAF) metrics "scorecard" at the request of the ISU exercise planners. At the strategic level, ADM (S&T) participated through the ADM Emergency Management Committee.

b. Exercises Supporting the ISU. The V2010 ISU's Vehicle Screening Area (VSA) and Pedestrian Screening Area (PSA) exercise campaign consisted of three exercises: Ex MOCKASIN, Ex BLUE, and Ex ICE. The ISU's Physical Security section welcomed and relied heavily upon DRDC planning, execution, and analytical support throughout its VSA and PSA exercise campaign. DRDC personnel played central roles with respect to each of the three exercises. In each case, DRDC personnel served as members of the core planning team, exercise controllers, data collectors, and as data analysts. The results of DRDC's exercise analyses provided an empirical,

quantitative basis for ISU's planning efforts, decision making, and discussions with VANOC. The contributions to the planning, conduct, and analysis of each exercise were very favourably received by the Physical Security and Private Security sections of the ISU. The resulting insights and advice spanned all aspects of VSA and PSA operations and helped prompt a paradigm shift in the ISU's VSA concept.

i. **Ex MOCKASIN** (June, 2008). The Mock Area Screening Exercise (Ex MOCKASIN) was conducted at the RCMP Pacific Region Training Centre in Chilliwack, BC during June, 2008. From a VSA perspective, the exercise explored the relative performance and requirements of a conventional design versus promising alternatives that arose from DRDC's modeling and analysis efforts. Time and motion studies were also conducted regarding the V2010 ISU's evolving PSA and Remote Vehicle Screening Site (RVSS) concepts. DRDC made essential contributions during the exercise planning phase by providing one member of the core, three-person planning team; advising on scheduling, resource, execution, and logistical issues; and designing the data collection plan. During the exercise's execution phase, DRDC provided key personnel, including the exercise's controller, its three-person data collection team, and one of two classroom instructors for participant training. DRDC also analyzed the exercise data and delivered its results to the V2010 ISU's Physical security section via a letter report as well as formal and informal briefings. The exercise methodology and data collection plan devised by DRDC proved to be highly effective and influential. The rigorously obtained results clearly illustrated (both quantitatively and qualitatively) that the alternative VSA approaches proposed by DRDC outperformed the conventional one during the exercise. Moreover, a strong stakeholder consensus regarding the relative suitability of each VSA option was engendered by enlisting many V2010 ISU and Vancouver 2010 Organizing Committee (VANOC) members (who would otherwise have been passive exercise observers) as vehicle occupants. The strength and clarity of the results and broad participant consensus fostered a paradigm shift within the V2010 ISU's VSA concept such that the conventional approach was supplanted by those proposed by DRDC. Consequently, the exercise strongly impacted all aspects of Game-time VSAs including their manning, spatial requirements, internal configurations, tent quantities and specifications, etc. Observations made during the PSA and RVSS portions of the exercise also prompted the V2010 ISU to revisit certain aspects of those planning efforts.

ii. **Ex BLUE** (January, 2009 – February 2009). Exercise BLUE (Ex BLUE) consisted of four real-world field trials: two VSA trials (held in Whistler, BC and Vancouver, BC) and two PSA trials (also held in Whistler, BC and Vancouver, BC). The exercise represented a larger scale, higher fidelity follow-on to Ex MOCKASIN whose participants included members of the V2010 ISU, VANOC, and the general public. During the exercise, the V2010 ISU's VSA and PSA concepts were tested under winter conditions at or near Olympic venues to identify potential gaps, improvements, and Games-time requirements in detail. DRDC's key contributions to the exercise included one member of its core, three-person planning team, the creation of its data collection plan, its exercise

controller, the seven-person VSA data collection team, the six-person PSA data collection team, and one of two classroom instructors for VSA participant training. In addition to their planned activities, DRDC personnel acted promptly to quantitatively address a fundamental question regarding magnetometer usage that arose during the Whistler PSA trial. To that end, DRDC personnel rapidly proposed, designed, conducted, and analyzed the results of an additional, impromptu magnetometer experiment during the exercise. DRDC analyzed the large bodies of data obtained from the VSA, PSA, and magnetometer field trials. The results were delivered to the V2010 ISU's Physical Security section in the form of three letter reports as well as formal and informal briefings. In general, the V2010 ISU made extensive use of the exercise's results when finalizing its Games-time VSA and PSA plans. Their impact was wide-ranging and encompassed aspects such as VSA/PSA screener training, manning, screening processes, tent structures, and equipment. The results of the impromptu magnetometer experiment were also highly influential. That is, they led the V2010 ISU to reconsider a prior decision concerning both its VSA and PSA concepts and to request DRDC's support for follow-on magnetometer work (i.e., Ex ICE). Ex BLUE's scale, locations, and high degree of realism also provided an excellent preview of numerous challenges that would confront Games-time VSA and PSA personnel during the following winter. Such foreknowledge was invaluable to ISU planners and DRDC personnel during the final planning and execution phases of V2010.

iii. **Ex ICE** (June, 2009). The V2010 ISU conducted the Instrument Configuration and Evaluation Exercise (Ex ICE) at its Richmond, BC headquarters during June, 2009 as a more comprehensive follow-on to Ex BLUE's impromptu magnetometer experiment. DRDC's key contributions included one member of the core, two-person planning team; the exercise's data collection plan; the exercise controller; one of its two data collectors; and one of its many test subjects. DRDC also analyzed the exercise data and delivered the results to the V2010 ISU in a formal briefing (a letter report is in preparation). DRDC's rigourously obtained, quantitative exercise results significantly advanced the V2010 ISU's understanding of magnetometer usage issues within the V2010 context. Consequently, they served to inform a subsequent V2010 ISU decision with important implications for Games-time VSAs and PSAs.

c. Pegasus Guardian Series. The PG series of command post exercises began in Nov. 2007, prior to MECSS, and resulted in four exercises in the series (PG1, 2, 2.2 and 3) leading up to V2010. Apart from PG1, the series was held in conjunction with the BRONZE, SILVER and GOLD exercises.

i. **PG1** investigated the processes required for information sharing in an integrated security unit in charge of public security for a major event. While conducted outside of the MECSS project, PG1 laid the foundation for follow-on integrated exercises that would call on MECSS for support.

ii. **PG2** was focused on the security pillar. Its aim was to examine and test information flows into, within and out of the ISU's Integrated Command Centre

(ICC) while affording participating organizations the chance to gain experience with operating together. DRDC provided the simulated C2 infrastructure for JTFG as well as analytical support to the ISU

iii. **PG 2.2**. PG2.2 was generated as a way to implement changes and also as a "warm-up" for SILVER which ran the week after. DRDC provided direct assessment and analysis support for PG2.2 to the ISU Exercise Planning Team. This success set the trend for all subsequent DRDC support to the V2010 Exercise Program. From PG2.2/SILVER on, the ISU drew its lessons learned and ways forward for the exercises almost completely from the reports DRDC supplied.

iv. **PG3** was the ISU's preparatory exercise for Ex GOLD. It was intended as a security exercise only in that the safety and games operations pillars were not heavily played or were played by surrogates. It was intended as the ISU's confirmatory exercise and was larger than GOLD in terms of the ISU's commitment of resources and effort. Similar to the previous exercises, it was intended as a way to confirm the readiness of the security architecture. DRDC provided support similar to the previous exercises but implemented the most robust assessment plan yet with more specific metrics and a set of confirmation criteria based on architecture frameworks work. A "scorecard" was developed at the request of the ISU which used a stoplight scoring to summarize DRDC assessment results. These results were of extreme sensitivity within the ISU which reflects the kind of impact and credibility that DRDC results had.

d. Marine Security Table Top Exercises. In support of the ISU's Marine Security Planning Team, members of the OMOC and the Federal Marine/Surface Technical Working Group, DRDC designed, developed, facilitated and assessed three carefully structured table top exercises (14-15 Oct. 2008, 13-14 Nov. 2008 and 16-17 Jun. 2009) known as Force Protection Matrix Game (FPMG) Marine One, Two and Safety/Security Matrix Game - Marine Three. These were all held at HMCS Discovery in Vancouver. Although each was unique in scale and scope, they were all aimed at improving the stakeholder's awareness of capabilities, resources, Standard Operating Procedures (SOPs), and areas of responsibility. The game structure came from an Australian methodology used for the first time in Canada at Marine One. The success of this first game resulted in the request for Marine Two and Three each of which employed methodologies that had evolved from the lessons of the previous game. Marine Three was the culmination of the methodology and enabled detailed evaluation of a large number of issues and efficient data capture. The V2010 Winter Olympic and Paralympic Games were supported by DRDC Defence Scientists from Esquimalt, Halifax and Ottawa who rapidly produced assessment reports that strongly influenced the marine security planning.

e. RCMP National Operations Centre Exercise. DRDC provided analytical support to two NOC exercises:

i. Incident Director's Course Table Top Exercise.

ii. Pegasus Guardian 2.2.

f. CBRNE. The decision was made by the Province to conduct a Live Play exercise as part of Exercise Gold to test first responder interoperability in response to a CBRNE event. DRDC supported BC IPS by designing, developing and delivering two live play exercises – a radiological event in Vancouver and a chemical event in Richmond.

g. Exercises Supporting Integrated Public Safety (IPS). In the aftermath of SILVER, IPS was aware of a number of gaps in the C2 planning between provincial, federal and security stakeholders. To try and bridge those gaps, they proposed a group of TTXs for the fall of 2009 and DRDC was asked to help facilitate some of them. All these TTXs ultimately made an important contribution to the preparations for the confirmation exercise at GOLD. The TTX's included the Safety/Security Integration TTX (16 Sept, 2009), the PREOC TTX (14 Oct. 2009) and a series of Venue TTXs. DRDC scientists (mostly the deployed SAs) provided planning, facilitation, data collection and analysis support for them. These TTXs were the first ones where DRDC suggested and demonstrated more formal data collection techniques which generated consolidated documentation of the results. These provided, for the first time, a common set of materials that the stakeholders could reference.

h. Exercises Supporting Joint Task Force Games (JTFG). The majority of JTFG training was conducted as an internally organized training series called Exercise Laurel Wreath (LW). JTFG conducted 12 distinct LW training events and 22 distinct training events. DRDC provided key initial training and exercise support to JTFG through the Joint Command Decision Support for the 21st Century Technology Demonstrator (JCDS 21 TD). The first time occurred when JTFG Headquarters (HQ) used the JCDS21 test-bed to mimic the Canadian Secure Network Infrastructure (CSNI) during the Pegasus Guardian I Experiment (PG1 Exp) held at the ISU on 18-23 November 2007. The second time occurred during JCDS21 Experiment 2 (EXP2) held in Ottawa during October 2008. That was followed by the JCDS21 support to EX Pegasus Guardian 2 (PG2) run during EX BRONZE on 12-14 November 2008. PG2.2 and EX SILVER Command Post Exercise during 9-13 February 2009 were the fourth time DRDC helped train and exercise the JTFG HQ. DRDC also provided some limited analyst support for LW 0907 and LW 1001 that are also summarized in separate annexes. During the fall of 2009 the DRDC analysis support was focused on ISU analysis needs. During EX PG 3, JTFG conducted a CF force readiness evaluation using live Air Command Centre (ACC) and Maritime Command Centre (MCC) forces under the name Ex SPARTAN RINGS .

2.9 Surveillance Domain

2.9.1 Marine

a. Marine. The majority of the work conducted in the surveillance domain was related to marine security. Early engagement by DRDC Atlantic staff allowed for the CF and the RCMP to fully exploit the knowledge and expertise gained through a number

of related research projects at DRDC. In particular, advice was provided in the following areas:

i. **Waterside security**. There was significant concern as to how to adequately protect a number of the venues with waterfront exposure. A number of letter reports were produced and delivered to the ISU providing options for security of these venues.

ii. **Long Range Acoustical Device (LRAD).** The RCMP was considering the purchase and deployment of LRAD devices to communicate with small boats. DRDC Atlantic arranged for an operational demonstration of a number of models and provided advice on employability. Because of this advice the RCMP made the decision that deployment of LRAD was not the appropriate device to meet their needs. Meanwhile, the LRAD demonstration at Ex Silver was used to inform the decision by the CF to use LRAD in an early deployment of a ship to Somalia in support of anti-piracy operations.

iii. **Diver Detection.** DRDC Atlantic has been conducting research related to improved methods for detecting divers under the Maritime Force Protection TDP and were well positioned to advice the marine security planning staff on options available. The work performed included an operational trial of the prototype diver detection system in Vancouver in cooperation with the CF. In the end, insufficient time, funding and personnel, meant the system was not deployed operational for V2010. The trial however did provide a great opportunity for both the scientists and the operators to explore the operational effectiveness of the new technology.

iv. **Automated Ship Image Acquisition (ASIA).** The CF requested access to high resolution cameras being used by DRDC Atlantic for the ASIA research project. This high tech equipment was deployed to Vancouver Island during V2010 as one element of the marine surveillance plan along with a night imaging system provided by the Canadian Forces Electronic Warfare Centre (CFEWC).

v. **Optimization of Patrol Boat Requirement**. The Marine planners of the V2010 Integrated Security Unit (ISU) requested an analysis on the requirement of patrol boats to defend the Burrard Inlet waterside Olympic venues. The study considered simple intercept geometries and number requirements to be on station at one time; more complex scenarios involving intruder avoidance, deception, chase and apprehension could have been done if more lead time had been available.

b. Other. In addition to support for marine security, the surveillance domain included other activities:

iv. **Radar advice**. Early in the project the RCMP put a tender out for a camera surveillance system for the venues. A potential bidder asked if they had considered radar instead of cameras. The RCMP Technical Operations team requested an expert on radar to explain the current advances in radar including

what it could and could not do in the scenario provided. A workshop was organized to provide the team with the required information.

v. **Link 16**. V2010 would be the first time that Canada would deploy its own Link 16 network for air operations (instead of joining the US Link 16 network). A scientist was deployed during Ex Silver to Esquimalt to work with the Link 16 team to explore the operational implications of this initial deployment.

vi. **Reach-back** advice was sought in two operational situations both involving potential interference from CF radar during the V2010 preparations

2.10 Psycho-social Domain

At the creation of the project Psycho-Social was defined as domain of work to be undertaken by MECSS. The only work done was the development of a state of science in the Psycho-Social domain that was created by Dr. Louise Lemyre of the University of Ottawa. This report was delivered to the CF LO. Because of the lack of a client at the ISU and the difficulties in contracting with the University of Ottawa, it was decided to not pursue additional work in the Psycho-Social domain. This decision was made for practical reasons; however it was believed that the psychosocial elements associated with the security of Major Events are significant, and warrant further research

2.11 Physical Security

The V2010 ISU employed Vehicle Screening Areas (VSA) and Pedestrian Screening Areas (PSA) to reduce the risk of vehicle-borne and person-borne prohibited items (e.g., weapons) entering V2010 venues. However, given the Winter Olympic and Paralympic Games' posture as a sporting event rather than a traditional security operation, it was important that VSAs and PSAs did not unduly delay the entry of vehicles and persons into V2010 venues. Moreover, given the sheer quantity and scale of such screening areas, significant fractions of the overall V2010 security workforce and budget were required to staff and fund them (i.e., several thousand personnel and more than 100 million dollars). Consequently, a careful trade-off between such planning considerations was sought during the VSA and PSA planning phases that would yield simultaneously effective, efficient, feasible, and cost-effective approaches. As starting points for its planning efforts, the V2010 ISU's Physical Security section adopted VSA and PSA approaches used during previous Olympic Games. However, official observers' anecdotal observations and media reports concerning prior Games indicated that such earlier approaches represented undesirable trade-offs with respect to effectiveness, efficiency, feasibility, and cost-effectiveness.

DRDC's support to the V2010 ISU's VSA and PSA concept development efforts began in September, 2007 (i.e., prior to MECSS' inception) and March, 2008, respectively. Initially, such support was jointly provided by single members of the DRDC CORA teams embedded at the headquarters of Joint Task Force Games (JTF-G; Esquimalt) and Canada Command (CanadaCOM; Ottawa), but was provided solely by the latter after March 2008. Over a 2.5 year period that included the Olympic Games, such full-time, continuous support expanded in response to a series of requests from the V2010 ISU. During that interval, DRDC provided a

large body of science-based advice that arose from two comprehensive VSA and PSA research and development campaigns. Described below, the campaigns included software-based model and tool development; short-deadline analysis; experimentation and field trials; and deployed troubleshooting support during the Olympic Games.

2.11.1 Software-Based Model & Tool Development.

DRDC developed three classes of software-based tools in support of the V2010 ISU's VSA and PSA efforts.

a. VISTA-VSA Process Model (September, 2007 – January 2008). DRDC's initial support to the V2010 ISU's VSA planning effort was proposed during a visit by the leader of DRDC CORA's embedded team at JTFG to the V2010 ISU in September, 2007. In a reach-back request accepted by DRDC CORA's embedded team at Canada Command, the JTF-P operational research team leader identified the need for a VSA process model. Such a model would be used to explore the requirements and implications of the existing VSA concept and to explore possible improvements to it. To keep pace with the operational tempo at the V2010 ISU, rapid development of the model was essential. Following a period of intensive development, a prototype was demonstrated to the V2010 ISU's Physical Security section in November, 2007. The model became operationally useful in January, 2008 and was known thereafter as the Vancouver Integrated Screening Team Assessment – Vehicle Screening Area (VISTA-VSA) model. It greatly advanced the V2010 ISU's quantitative VSA planning capabilities and enabled rapid options analyses during the early days of the planning effort. In particular, the model served as a key enabler for influential analyses of V2010 ISU and VANOC planning data during February and March, 2008. It was also used to identify the promising VSA concept alternatives that formed the basis of the V2010 ISU's VSA exercise campaign. VISTA-VSA's modular program code was designed to facilitate the rapid creation of a family of analogous VISTA process models requested by the V2010 ISU (i.e., VISTA-PSA and VISTA-RVSS for V2010 Pedestrian Screening Areas and Remote Vehicle Screening Sites, respectively). To that end, VISTA model development continued into May, 2008 until it ceased due to the receipt of higher priority support requests from the V2010 ISU.

b. PSA Calculator Tool (September, 2008). DRDC's development of the VISTA-PSA process model ended when an internal V2010 ISU deadline for PSA requirement identification was unexpectedly brought forward. In response to the now-urgent need for a PSA planning support, DRDC rapidly developed a system of equations to approximate PSA operations under certain best-case conditions. These were implemented in a Microsoft Excel spreadsheet-based tool named PSA Calculator whose prototype and final versions were delivered to the V2010 ISU two and four days, respectively, after the support request was made. Although less capable than a full process model (such as the planned VISTA-PSA), PSA Calculator immediately became a key V2010 PSA planning tool. In particular, the tool was used extensively by the V2010 ISU's Private Security section to explore all aspects of the evolving PSA concept, including potential screening process modifications as well as estimated requirements for personnel, equipment, tents, and space.

c. DANTE Data Acquisition Software (August, 2009). During VSA and PSA exercises, DRDC personnel recorded a multitude of quantitative data by hand. Although effective, such approaches typically proved to be demanding for data collectors due to the fast pace of collection, the large volume of data, and the need to devote multiple hours at the end of each day to electronic data entry and validation. In anticipation of a V2010 ISU request for DRDC to collect such VSA and PSA data during the Olympic Games, DRDC devised a general approach for all-digital, touch-based data collection using netbook tablets. Known as Data Acquisition via Netbook Tablet Entry (DANTE), two software implementations of the approach were developed for potential Games-time use (i.e., DANTE-VSA and DANTE-PSA). Informal tests indicated that the approach could greatly facilitate data collection, improve its accuracy, eliminate the need for time-consuming data entry and validation, enable real-time data analysis, and better inform troubleshooting efforts. However, since the V2010 ISU did not issue the anticipated high-level request for Games-time data collection, DANTE was not field-tested extensively during the Olympic Games.

2.11.2 Short-Deadline Analysis

a. VSA Manning & Capacity Estimates (February, 2008). In response to an urgent request by the Canadian Forces (CF), two DRDC CORA personnel conducted a detailed analysis of existing VSA planning data at the V2010 ISU's headquarters in Richmond, BC, during February, 2008. The analysts examined the internal consistency of existing resource estimates then used them, in conjunction with the VISTA-VSA model, to estimate the consequent vehicle screening capacities at various V2010 venues. VISTA-VSA was also used to identify potentially promising modifications to the existing VSA concept and to quantify their impact on the estimated performance of particular VSAs. The analytical results were highly influential in two respects. First, they informed a key Canadian Forces decision on whether to provide CF personnel for the purpose of Games-time vehicle screening. Second, the results provided a strong example of the highly responsive and relevant analytical support that DRDC could provide to the V2010 ISU. This represented a major milestone in the establishment of the DRDC/V2010 ISU relationship and soon precipitated additional V2010 support requests, including those for PSA modelling and its VSA and PSA exercise campaigns.

b. Analysis of VANOC VSA Traffic Estimates (March, 2008). The performance of a particular VSA depends on a great many factors. Thus, planners require access to a wide range of good quality planning data in order to design well-functioning VSAs for each venue. Although the V2010 ISU's Physical Security section could generate planning estimates for many key data types, it was reliant on VANOC to provide it with others. During March, 2008, two DRDC CORA personnel used the VISTA-VSA process model to analyze two distinct sets of vehicle arrival estimates provided by VANOC. The results were briefed to members of the V2010 ISU and VANOC and comprised a vivid, quantitative illustration of the VSA planning process' need for rigorously generated, self-consistent, and accurate planning estimates. The

importance of good quality VSA planning data was also highly apparent during the Olympic Games.

2.11.3 Experimentation & Field Trials.

Throughout its VSA and PSA exercise campaigns, the V2010 ISU welcomed and relied heavily up on DRDC's comprehensive planning, exercise control, data collection, and analytical support. DRDC's experimental expertise and commitment to objective, rigourous analysis were seen by the V2010 ISU's Physical Security and Private Security sections as having been highly beneficial to their VSA and PSA planning efforts. In particular, DRDC exercise analyses provided empirical, quantitative bases for the V2010 ISU's decision making and discussions with VANOC and also fostered a paradigm shift in its VSA concept. The details of these exercises are included in the Exercise section of this Report.

2.11.4 Deployed Games-Time Support (February, 2010)

a. VSA & PSA Troubleshooting. One DRDC CORA analyst was deployed the Olympic theatre to provide VSA and PSA troubleshooting support to the V2010 ISU's Physical Security section throughout February, 2010 (i.e., prior to and during the Olympic Games). Typically operating in the field alongside a Physical Security section member, the analyst provided timely, site-specific advice based on pre-Games modeling, prior exercise results, and Games-time observations made at twelve venues in vicinities of Vancouver, BC and Whistler, BC. DRDC's advice was consistently sought by the Physical Security section regarding its highest priority VSA/PSA issues and operations. Deployed support included the provision of advice regarding the time-sensitive redesign or reconfiguration of specific areas and processes, consultations with venue and VSA command staff, problem forecasting, and the creation of venue-specific aides-mémoire for VSA personnel.

b. VSA & PSA Data Collection & Analysis. During June, 2009, the V2010 ISU's Physical Security section informally expressed its desire for DRDC to lead rigourous data collection efforts for Games-time VSAs and PSAs akin to those conducted during Ex BLUE. Such data would have had considerable value for Games-time troubleshooting purposes, would have provided useful VSA and PSA performance measures (particularly for the novel VSA approaches used), and would have served as important references for planners of future events such as Toronto 2015. Given the many likely benefits, the Physical Security section recommended that the V2010 ISU's senior management formally request such support from DRDC. In anticipation of such a request and given the long lead time required, DRDC devised plans for a joint VSA/PSA Games-time analysis team and created the DANTE data collection methodology to meet the Physical Security section's informal requirements. Many months later, in December, 2009, the senior management of the V2010 ISU elected not to request such support from DRDC, then reconsidered and undertook to inform DRDC of a final decision to be made in early January, 2010. However, DRDC was not subsequently informed of any such decision and, consequently, no detailed VSA or PSA data collection of the sort recommended by the Physical Security section was conducted at Games-time. Such data, had they been collected as recommended,

would have readily answered a fundamental VSA-related question that arose during V2010 and generated much discussion within the V2010 ISU. Planners of future major events (such as Toronto 2015) will likewise be deprived of the significant benefits that such data would have provided. Given that VSAs and PSAs constitute major cost drivers within the security budgets of such events, the lack of such data may have significant, negative cost ramifications in the future. Prior to the stand-up of the MECSS project, regular visits to the embryonic V2010 ISU from September, 2007 to March, 2008 by the leader of DRDC CORA's embedded team at JTFP/JTFG were instrumental to DRDC's wide-ranging VSA and PSA support. Such interactions were key to the establishment of the DRDC/V2010 ISU relationship and resulted in the early identification of VSAs as a major area for DRDC support. The subsequent embedding of a DRDC scientific advisor within the V2010 ISU yielded both a vital source of situational awareness and a secondary communication channel for the VSA and PSA work.

The February, 2008 analysis of VSA manning and capacities was regarded by many V2010 ISU members as a vivid demonstration of DRDC's ability to deliver timely, rigourous, and highly relevant quantitative analysis in support of V2010 VSA planning. Consequently, it underpinned the excellent working level-relationships built subsequently between DRDC and the V2010 ISU's Physical Security and Private Security sections. Such strong relationships were furthered by DRDC scientific staff's regular provision of analytical results and site visits. The importance of the trust engendered by each successive interaction to the VSA and PSA support efforts cannot be understated. As the relationships strengthened, the quantity and importance of requests for VSA and PSA support increased, as did the likelihood that the resultant knowledge and advice would be adopted by the V2010 ISU's working-level personnel.

A request for DRDC to conduct quantitative analysis as part of its Games-time troubleshooting activities was staffed through the ISU to the senior leadership. The request was not supported. The lack of quantitative data hampered Games-time troubleshooting and prevented the accumulation of real-world VSA and PSA data that could have been enormously useful to planners of future major events.

Overall, the outcomes associated with VSA and PSA support to the ISU is heralded as a profound success. This support is a showcase example of how the rigour of S&T can directly impact the effectiveness and efficiency associated with the delivery of security at Major Events

2.12 Cyber

Cyber was not a MECSS domain and did not have a designated lead as part of the MECSS project; however, the SA IPS had expertise in cyber security as a former scientist with the Network Information Operations section of DRDC Ottawa, and undertook a project in this area after identifying gaps in preparations.

The cyber events in the 2010 Exercise Series were limited in scope and participating agencies and did not fully test the exercises objectives. Leading up to V2010, the emergency management community represented at the Regional Integrated Exercise Working Group expressed limited interest in cyber (for example, the province of BC did not participate in the cyber component of

the exercises). As a result, the federal group under the 2010 Cyber Security Working Group took a lead in designing the cyber incidents and the scenario development was targeted for the RCMP and DND for Exercise Silver. The focus was significantly broadened for Exercise Gold and an invitation for participation was extended to all organizations; however, outside of federal government departments, few organizations chose to participate. VANOC was encouraged to lead a cyber incident for Exercise Gold, but, despite interest from partners, the incident was contained within VANOC and did not result in any loss of service.

The situation observed as of the summer of 2009 was the following:

- The federal V2010 Cyber Security Steering Committee/Cyber Security Working Group realized the importance of the delivery of government services for V2010 on IT infrastructure and compiled a report on participating federal departments based on self-assessment surveys. High-level recommendations were made and departments were responsible for identifying cyber preparedness gaps and mitigating or accepting the risks.

- An overall cyber threat and risk assessment had not been performed for V2010, although there was a misperception that a full analysis has been undertaken.

- Most cyber security work was being done in silos.

- No organization was examining cyber preparedness across key public and private sector games stakeholders.

A discussion on cyber security between DND ADM(S&T) and senior ISU staff in July of 2009 and the support of the ISU CF LO were instrumental in getting the MECSS task pertaining to Cyber off the ground. A project team was created, consisting of the IPS SA, a research engineer from DRDC Ottawa Network Information Operations (NIO) Section, a member of Chief of Defence Intelligence - Computer Network Operations, the security representative of the ISU Informatics group, and, initially, a member of CSIS. The Canadian Cyber Incident Response Centre (CCIRC) was engaged but resources were not available to participate in some of the initial discussions. In light of varying levels of support from some offices, the project kept a low profile and work was focused at the operator level. Within the operator community, support varied by organization but most people were generally very willing to share information.

The team identified key cyber stakeholders for V2010 as the ISU, DND, the Province of BC, VANOC, E-Comm, and Bell. When the distribution of a standard cyber security audit checklist in August-September 2009 yielded a poor response (likely due to a lack of time and resources), face-to-face interviews were held with each stakeholder organization to collect relevant data. A summary report on key observations and recommendations was provided to the ISU based on the information provided in interviews.

A key cyber stakeholder contact chart was developed for information sharing and incident response. This typically included a 24/7 network/security help desk contact and key cyber security contacts, such as those interviewed as part of the security review, as well as Industry Canada (IC) and CCIRC contacts. Both CCIRC and IC were engaged to establish the reporting process from the private sector organizations. IC was the point of contact for Internet Service

Providers and had pre-established relationships, information sharing agreements, and reporting processes already in place.

The NIO engineer supporting the project became the CCIRC Chief of Cyber Operations at the beginning of February 2010. This was very timely since he was able to facilitate the establishment of CCIRC as a trusted agent for the key Games stakeholders. During the Olympics, CCIRC hosted regular cyber conference calls among the stakeholders, and the group collectively chose to extend the conference calls into the Paralympics. Information sharing resulted in increased situational awareness across stakeholders. As anticipated, VANOC was a target during the Olympics and reported information on various attacks. Organizations collaborated in addressing issues/problems, crossing federal, provincial, and private sector boundaries. This ability to rapidly share information, access cyber expertise across private and public sectors, and respond to events was collectively much more than any agency had on their own.

Overall, the cyber security would have benefited from stronger centralized coordination and leadership within cyber domain. One outcome of the support to cyber security is recognition that Canada needs a national entity to provide due diligence for cyber security for major events: to build and maintain trusted relationships across sectors, perform appropriate threat and risk assessments, identify and mitigate gaps, facilitate information sharing, and establish and exercise a cyber response capability across stakeholders.

2.13 Major Events Security Framework

Canada's experience and associated challenges with security preparations for V2010, G8 and the G20 have illustrated opportunities for a stronger alignment of planning activities across the domestic security domain. Challenges associated with integrated planning, communications, and interoperability, can be attributed to dissimilar organizational cultures and planning doctrine. The existing challenges are compounded by a national safety and security infrastructure that is challenged to fully exploit collective learning opportunities between agencies and across jurisdictions. This circumstance denies the national security domain the opportunity to embrace the lessons from past Major Events and to deliver a progressively improved integrated security solution. In support of the RCMP, MECSS undertook the development of Major Events Security Framework that is intended to serve as:

- A planning forum that integrates 'whole of government' collaborative planning for security operations;
- A knowledge management system that identifies best practices, captures lessons, effects change, and champions innovation;
- A repository of value-added tools and technologies;

Development of this RCMP framework has progressed along four main themes: creating the foundation; identifying technical solutions; capturing the planning process; and building the solution.

To contribute to the foundation of the framework, the University of Victoria, under contract, conducted research with the following scope:

- Surveyed of the available literature on major events safety and security operations;

- Studied the implications of Canadian legislative, policy and jurisdictional frameworks on the governance and execution of major events safety and security operations;
- Identified organizational and management teachings that would support the effective governance and execution of major events and major events safety and security operations;
- Recommended a synthesis of the principal components of a best-practice framework.

In addition to the final report from this effort, a companion document was prepared focusing on Major Events Security Framework Information Sharing and Knowledge Management. The report describes how information could be handled in a collaborative Decision Support System (DSS) used in support of Major Events planning and preparation. The final reports that stemmed from this research informed the development of the MESF by providing a foundation within the organizational and management literature.

A contract was concurrently established with Fujitsu through the JCDS 21 contract mechanism to conduct a framework options analysis that would realize the key characteristics of the framework. During the course of this research GCPedia emerged as a preferred option to connect the planning processes as it satisfied connectivity across the federal government departments and supported a collaborative workspace suitable for the evolution and conduct of integrated planning.

During the course of this work, over 40 workshops were facilitated that brought together stakeholders and subject matter experts from the RCMP and DRDC. During the course of these workshops, the functional requirements were gathered through the iterative rapid development of a prototype model.

The final phase is the population of the data into GCPedia. Through active liaison, Treasury Board (GCPedia host) became fully engaged and supportive of this project. They agreed to support the GCPedia roll out of the MESF by hosting students, hired through FSWEP, at their office and help facilitate the development of the framework.

Post MECSS, the activity associated with the development of the MESF will be transferred to a MESF project that will be set up under the Public Security Technical Program, as managed by DRDC Centre for Security Science. The Project will be funded to cover further development, implementation, as well as maintenance to end FY2011.

2.14 V2010 Deployment

Operational Deployment: In support of V2010, MECSS deployed a broad range of science expertise and equipment in support of V2010. This ranged from individual scientific expertise and specific operational equipment, to full-up capabilities such as the CBRNE laboratories that were deployed within Science Town in support of the RCMP National CBRNE Response Team. DRDC resources were deployed under the authority of the ADM(S&T), as directed through the DRDC V2010 Operational Directive. The Senior Military Officer at CSS (also Project Director) was assigned to coordinate and lead the deployed operations. S&T support from outside DRDC was coordinated through a variety of agreements and MOUs. In regard to the deployment of

Science Town in Vancouver and Whistler, the authority to coordinate was delegated to ADM(S&T) by the Deputy Minister V2010 Security Advisory Committee. MECSS also coordinated a 24/7 reach back posture for the duration of security operations (23 Jan-28 Feb). The deployment was planned through an operational planning process that was modified to suit the limitations and constraints inherent within DRDC. The Operational Deployment was delivered through each of the DRDC Centres, with strong centralized support from the MECSS project.

During the Operational Period, DRDC established an operational tempo to accommodate the effective delivery of S&T support, as well to ensure ADM(S&T) was prepared to fulfill his S&T advisory position within the ADM Emergency Management Committee. Daily reports and returns from each of the DRDC OPIs provided a suitable degree of situational awareness to ensure S&T support was being effectively delivered. As well, these reports and subsequent daily briefings to the ADM (S&T) satisfied his requirements to support the ADM EMC and Departmental responsibilities as ADM (S&T).

This was the first deployment of this magnitude for DRDC personnel in support of a domestic security operation. Much was learned across the agency. Many of these lessons were applied in the planning and execution of support to the G8 and G20.

2.15 G8/G20 Support

A defence scientist, from DRDC Toronto, was deployed as the Scientific Advisor to the Summits Integrated Security Unit located in Barrie, ON. The specific lessons learned from his deployment are available as a separate technical report. The decision was made at the SRB that support for G8/G20 would be limited to exploiting work done for V2010 and that no new work would be undertaken. Due to delays in getting the SA into the ISU and to the main effort being V2010, the support provided to G8/G20 planning was limited to the provision of advice in the following areas:

a. Shift Scheduling,

b. VSA/PSA,

c. Marine Security,

d. Command and Control,and

e. Exercise Support.

DRDC Support during the actual events was more extensive and included the following elements:

a. Mobile Chemical lab (plus team) in Toronto for the G20,

b. Mobile Radiological-Nuclear lab (plus tech in Huntsville for the G8,

c. C2 Analysis team supporting knowledge management and lessons learned both the G8/G20,

d. PSA trouble-shooting support in the Toronto area,

e. Logistics support at DRDC Toronto for the RCMP Mobile Command Centre and the Joint CF/RCMP Air Component, and

f. Scientific Advisor at the RCMP National Operations Centre, the Government Operations Centre and at the ISU in Barrie.

2.16 Schedule Performance Summary

The planned and completed milestones were the following:

Milestone	Planned Completion Date	Actual Completion
Project Initiation	26 Feb 08	26 Feb 08
Project Approval	3 May 08	3 Apr 08
Develop/Exercise Phase	31 Dec 09	31 Mar 10
Conduct Phase	31 Mar 10	31 Jun 10
Project Completion	31 May 10	1 Aug 10

Table 1 : Milestones

The schedule variance was due to a change in scope to add support during the G8/G20 exercises in Ontario at the end of Jun 2010.

2.17 Cost Performance Summary

($000 BY)	FY 07/08	FY 08/09	FY 09/10	FY 10/11	Total
DRDC Agility Fund	25	4327.8	2809.8	299.6	7462.2
CRTI		370	650		1020
PSTP		230	340	40	610
Total	**25**	**4927.8**	**3799.8**	**339.6**	**9092.2**
Contingency		492.78	379.98	33.96	906.72
Total Project Cost	**25**	**5420.58**	**4179.78**	**373.56**	**9998.92**

Table 2: Original Cost Breakdown - approved 5 May 2008

($000 BY)	FY 07/08	FY 08/09	FY 09/10	FY 10/11	Total
DRDC Agility Fund	25	2997	2419	272	5713
CRTI			2455	480	2935
PSTP					

Total	**25**	**2997**	**4874**	**752**	**8648**

Table 3: Revised Cost Breakdown - approved 6 Apr 2010

Final Project Cash Flow

($000 BY)	FY 07/08	FY 08/09	FY 09/10	FY 10/11	Total
DRDC Agility Fund	25	2997	2419	204	5441
CRTI			2455	33	2488
PSTP					
Total	**25**	**2997**	**4874**	**237**	**7929**

Table 4: Actual Cost breakdown

Canada Command allowed for G8/G20 expenses totalling $180,708.17 to be expensed against the Memorandum to Cabinet funding allocated to DND for the G8/G20 Summits.

2.18 Leveraged Activities

Project	Nature of Contribution
RCMP ME&PS	Louis Chaisson played a key role in building existing content in the Major Events Framework
CBRNE Mobile Labs	CRTI Technology Acquisition Project provided the mobile labs for Deployment and covered limited deployment costs.
JCDS 21 TDP	During the first year of MECSS, many of the resources were provided from the JCDS 21 TDP. MECSS exploited exercise scenarios, DNDAF models and the JCDS 21 testbed was used during Ex Bronze by JTFG. The project also made extensive use of the JCDS 21 Integrator contract and other Standing Offers.
Air Force OR	Much of the Air Force OR work was done directly for the CF client and not through MECSS.
Maritime Force Protection TD	This Technology Demonstration Project (TDP) provided the Diver Detection equipment that was trialed in BC. In addition, many of the low technology solutions recommended by the TDP were in fact adopted by the operators.
ASIA TDP	The high resolution camera portion of the ASIA system was deployed to Comox during V2010
LRAD	The LRAD system was demonstrated in BC by DRDC Atlantic Maritime Force Protection TDP.
CATSI	The Compact Atmospheric Sounding Interferometer Engineering Development Model (CATSI) equipment from DRDC Valcartier was deployed to Victoria in stand-by mode during V2010.
METER CBRNE Training	Three separate CBRNE courses were provided to first responders in BC.
TTCP AG-10	MECSS was able to leverage previous The Technical Cooperation Panel (TTCP) Action Group (AG-10) work on the Force Protection Matrix Game

Table 5: Leveraged Activities

3 RECOMMENDATIONS FOR FOLLOW-ON ACTIVITY

3.1 Transition of Project Products into Operations

a. Science Town. Science Town has been a showcase success at the Olympics, G8, and G20. Despite the degree of success, the concept is still young and requires a formal framework be developed to ensure it can be employed effectively in the future. DRDC CSS has taken on the task of working with the many departments to develop a scalable framework for Science Town and associated Concept of Operations. This will include the facilitation of decisions to determine how Science Town will fit into the broader policy and mandate framework within Government. It is recommended that DRDC CSS continue to support the integration of Science Town within the RCMP National CBRNE Response Team.

b. Clandestine Lab. As part of the CBRNE training of first responders MECSS supported the construction of a clandestine lab in Vancouver. This clandestine lab was built by the Vancouver Fire Department and will support ongoing CBRNE training in the area.

c. C2 portal for Command View. The work done by DRDC Valcartier was immediately put into service by the JTFG J6. The intent is for the architecture, portal and the resulting information to be part of any CIS deployment.

d. Critical Infrastructure Support to the Province of BC and PS. The Deputy Minister of Public Safety and the Solicitor General has requested, in a formal letter, follow-on support from DRDC in the realm of Critical Infrastructure. This requested support is, in part, considered an extension of the work that had been provided to BC in support of V2010 safety and security. DRDC CSS, with Departmental oversight, has worked out an agreement with Emergency Management BC, and is continuing to provide support to the Province.

e. Scientific Advisor in RCMP. An agreement has been reached with the RCMP for CSS to continue to provide a Scientific Advisor over the next year.

f. Operational Analysis. In May 2010, the leadership from the G8/20 ISU called on DRDC to provide analytical support to the ISU Knowledge Transfer Plan (KTP). The KTP seeks to accommodate a significant transfer of knowledge to support future security events of this magnitude. A reach-back request was made for DRDC to provide operational analysis support during G8/20 operations. During operations, DRDC teams were tasked with conducting interviews with key members of the security delivery organizations. The ISU leadership felt that many of the issues that typically go ‘unaddressed’ during these types of security operations could be captured by having access to real time interview capabilities. DRDC Toronto took the lead with this activity and developed a posture suited to cover the span of operations between Huntsville and Toronto. Borrowing on the credibility earned through the Exercise Program, the teams were well received with unprecedented

access to security personnel during, and post, operations. Teams from DRDC Toronto will remain engaged with the ISU until Dec 2010, to finalize the interviews and the associated analysis.

g. After Event Review. In the fall of 2009, the Office of the Coordinator for the Security of the Olympics and G8 (OCS) requested DRDC support in the conduct of the OCS Closeout Report. With endorsement from DND leadership, DRDC CSS created a separate project under PSTP to accommodate the activities associated with a rigourous scientific review of specific elements associated with V2010 security. The After Event Report (AER) focuses on issues from a whole of government perspective, with emphasis on gaps and best practices. The report summary and recommendations were presented to the V2010 DM Committee on 8 Sep 2010, while the final report was delivered to the OCS on 27 Sept 10. It is the intent of the OCS, Mr Elcock, to provide the AER to the National Security Advisor.

h. Major Events Framework. The Framework has been successfully implemented into the GCPedia environment and final reviews are being conducted before it goes live. The lessons learned collected from the G8/G20 will find a home in the RCMP Major Events Framework.

i. Reports. To date, more than 195 reports have been generated for V2010 and MECSS. A large number of other reports are still being written. A bibliography listing is included in Section 5.

3.2 Follow-On R&D Projects Recommended

Despite all of the work accomplished during MECSS, there were a number of areas that either did not achieve sufficient maturity or could not address the entire scope of the problem. The following are areas that MECSS believes require additional R&D investment:

a. Mobilization. One of the biggest problems facing the security community, and one of the largest cost drivers, is the ability to obtain and move large numbers of law enforcement personnel. This problem was observed during V2010 and again during the G8/G20. For most major events, an influx of labour will be required to provide security. The problems facing the planners include sourcing appropriate skillsets, logistics (movement, housing, equipping, feeding) and shift scheduling. During V2010, some work was done on developing a shift schedule; however this is just a small portion of the challenge facing the physical security planners.

b. Diver Detection. Both the V2010 Olympics and Paralympics and the G8/G20 had a significant marine component. A recurring problem involves how to discreetly protect against waterborne threats including underwater divers. The DRDC Atlantic Maritime Force Protection TDP has made great progress in exploring options however additional work is needed to address the needs of internal waterways and the public security community.

c. Waterside Response. Waterside response and interdiction is a significant issue in Canadian waters, especially in regards to non-lethal weapons and non-lethal warning

technologies that have the potential to be used as non-lethal weapons. This is another area that was investigated through the MFP TDP, but much work remains to be done, including in regards to Environmental assessments, and legal uses/Rules of engagement.

d. Underwater Blast Modeling. We also noted a lack of national capability in the modeling blast effects on underwater structures. Though models are available for modeling blast impacts on ships (in particular military ships) and expertise does exist to extend these codes to underwater structures such as piers and pylons, these models do not currently exist.

e. Psycho-Social. There are a number of best practices in regard to Community Engagement leading up to and during the Olympics that significantly contributed to the outcomes of the security posture for V2010. Despite this, from an S&T perspective, there remains a limited volume of academic or scientific literature to support operational decisions in terms of the psychosocial elements that impact events of this nature and magnitude. There is a sense that a greater depth of understanding pertaining to the psychosocial elements of a community hosting a major event, will significantly contribute to more robust security planning and plans in terms of community engagement. It is recommended that this be considered for future research projects.

f. Organizational Cultures in Public Safety and Public Security. The role that culture plays in a whole of government domestic security is beginning to be understood. There are already a number of projects in DRDC looking at various aspects of the problem.

g. Surveillance Options. Perimeter security is a significant and often costly capability for Major Events, which has been traditionally resolved through highly technical fencing and integrated surveillance systems. At the outset of MECSS, there was an informal request for DRDC to consider surveillance options to support decisions pertaining to the Perimeter Intrusion Detection System (PIDS). MECSS did not get engaged as the RCMP Project to satisfy the PIDS requirements was already mature and out as a Request for Proposal. Although the RCMP is well experienced with this type of technology, in the future it would seem that stronger ties with DRDC surveillance expertise could contribute to informed decisions pertaining to the spectrum of surveillance options

3.3 Intellectual Property Disposition

The focus of the MECSS project was on exploiting previous R&D therefore it did not generate a large body of intellectual property. There were four areas where items of potential value were created. In each of these cases, the technical authority was advised to explore with DRDC Corporate whether or not it would be appropriate to register patents against the work. There are no circumstances where there were plans to license the intellectual property to industry.

a. I2Sim. Four working copies of the I2Sim model were delivered to DRDC. Background IP remains with UBC (Paul Chouinard is Technical Authority)

b. VSA and PSA Models. All IP rests with DRDC (Patrick Dooley is Technical Authority).

c. Shift Scheduling model developed in ILog ODM. All IP rests with DRDC (Alan Hill is Technical Authority)

d. C2 portal. This work was done in-house and is being used by the CF (Adel Guitouni is the Technical Authority)

3.4 Disposition of Project Products

A portion of the MECSS funding went to equipment or tools to support the MECSS teams or develop solutions for the clients. The following items of value were purchased:

a. Laptops. Eight laptops were purchased for use by the MECSS team including the deployed Scientific Advisors. All of the laptops will be retained on the DRDC Corporate inventory with the exception of the laptops used by Ron Funk that will be transferred to CORA;

b. Netbooks. Three netbook computers were purchased by MECSS for use by Patrick Dooley during V2010 to support data collection. These netbooks have been loaned to DRDC Toronto for use supporting the G8/G20 lessons learned capture. These netbooks will be returned for retention by CORA;

c. I2Sim. As part of the contract with UBC for I2Sim, four copies were installed on MECSS laptops. The I2Sim software includes 3rd party software of Matlab and Simulink. The licences will be distributed as follows after MECSS: 3 for CSS and one for CORA;

d. C4ISR Mobile lab. The DRDC Valcartier asset was transferred to JTFG for their use during V2010 (followed by JTFC for G8/G20). The C4ISR mobile lab has since been returned to DRDC Valcartier;

e. JCDS 21 Equipment. In support of Ex Bronze, DRDC shipped a large quantity of equipment to Vancouver. Following Ex Bronze, this equipment was delivered to JTFG in Esquimalt. DRDC Valcartier has received financial compensation for the equipment retained by JTFG and some has been returned to DRDC Valcartier;

f. ASIA Spares. MECSS provided funding to DRDC Atlantic to purchase spare equipment in support of the deployment of the ASIA camera to Vancouver Island. These spares will be retained by DRDC Atlantic;

g. Diver Detection Spares. MECSS provided funding to DRDC Atlantic to purchase spare equipment in anticipation of the deployment of the Diver Detection Equipment.

Although the equipment was not used during V2010, DRDC Atlantic will retain these spares;

h. Chemical Detectors. MECSS purchase 6 chemical detectors to enhance provincial capability during V2010 and an additional 3 for use by the Chemical Cluster. These chemical detectors will be held on the CSS Supply Customer Account however 6 have been loaned to the Province of BC for an indefinite period of time;

i. CBRNE Ex Gold Equipment. MECSS purchased a variety of miscellaneous equipment to support the scenarios used during Ex Gold. This equipment was given to DRDC Ottawa for their use or disposal;

j. Science Town Equipment. MECSS purchased a small fridge and microwave for use by the employees located at the Science Towns during the V2010 deployment. The equipment located at Whistler has been retained by DRDC Suffield while the equipment at Vancouver was given to the reserve unit located at the Seaforth Armouries in Vancouver;

k. Science Town Internet Equipment. MECSS purchased all of the equipment required to provide internet access at the Seaforth Armouries in Vancouver. This equipment has been transferred to Natural Resources Canada who has agreed to make it available for future deployments of Science Town;

l. Clandestine Lab. MECSS provided funding to create training facilities at the Vancouver Fire Department. The Vancouver Fire Department was able to build a dedicated clandestine lab that will be retained to support future CBRNE training, and

m. Miscellaneous Equipment. All additional equipment purchased by MECSS will be retained by CSS (digital camera, digital video camera, in-focus projector, voice recorders, stop watches, measuring tapes, CO2 detector)

3.5 Policy or Procedural Changes

The MECSS project represented the first time DRDC provided extensive S&T support to a domestic security operation. Through the planning and execution of support to V2010 and G8/G20, work was done to develop/enhance DRDC policies for domestic operations. Work is still required on the following policies:

a. Deployment of Civilians. A new policy was generated to deal with deploying civilians for domestic operations. This policy needs to be reviewed and enhanced based on the V2010 and G8/G20 experiences. In particular, more clarity is required on the policy on overtime, the applicability of 'field work' for DS and the issue of dangerous situations;

b. Travel Status. DRDC frequently sends DS on assignments to other Centers, however MECSS sent two employees on assignment to a location where no embedded administrative support exists. Better clarity of the travel directive as it applies to such situations is needed to avoid future conflict;

c. Reach-back/Tasking Process. MECSS generated a tasking process that used the DDG/SMO network. Post MECSS, the need remains for a process to task Centres, when appropriate, to contribute to events such as operations and exercises. The process used for MECSS should be reviewed to determine its suitability for becoming a standard operating procedure within DRDC;

d. Use of Information Request Manager. This tool was generated under an R&D project and has been in use by the CF for a number of years. It has also being implemented at Public Safety Canada to support the tracking of reach-back requests with the Emergency Operations Centres. DRDC has implemented IR Manager on the DRDC Network and it was used centrally by the MECSS team for V2010, but not for G8/G20. While not used to its full capacity, because it was used, we have a full listing of the requests for S&T advice and answers provided. This same tracking does not exist for the G8/G20. The IR Manager should be fully implemented across DRDC to support requests for S&T advice. In addition, DRDC should get an account on the CSNI version of IR Manager to support classified requests; and

e. Support to Domestic Security Operations. DRDC support to V2010, G8, and G20 was declared a priority activity by ADM (S&T); therefore, the DRDC Centres were required to compromise ongoing work and give priority to the operational needs of MECSS. Support to MECSS was a challenge for many of the Centres as much of the MECSS support activities were unforecast, and not built into the Centres' annual business plan. The practice of interrupting long term S&T activity in order to address unforecast short term operational needs is unsustainable within the existing DRDC structure. If DRDC is to continue to support domestic public safety and security operations in the longer term, then there is a requirement for a more formal process that attempts to forecast operations and exercises that will require S&T engagement, and then appropriately align this activity within the DRDC business planning process.

4 LESSONS LEARNED SUMMARY

4.1 Project Director's Observations

The MECSS Project had a very broad scope that fully engaged several science domains, and spanned a number of agencies and jurisdictions. There is much to be learned from this experience. As the Project Director my comments will first focus on strategic elements, which offer new knowledge and insight that will be of value to those engaged in the support of future major events. The comments will then focus on three primary areas that are Project related: Set-up, Execution, and Legacy.

The MECSS Project's 'centre of gravity' was the trusted relationships that it was able to achieve and sustain with each of the security delivery organizations. These relationships were key elements in understanding and articulating the operational requirements. As well, they facilitated the exploitation of the science as it was delivered to the security partners. Without these relationships, the MECSS Project would not have achieved the level of success that it did. The following comments should be considered within the context of this primary factor.

4.1.1 Strategic Considerations

Given the nature and profile of this project, the Director was regularly exposed to a variety of strategic forums which highlighted many key challenges facing Departmental leadership. The following issues reflect topics that were of concern within the strategic domain.

Organizational Culture and Doctrine: The difference in organizational cultures across the safety and security spectrum is healthy and can contribute to a very positive collaborative environment. The integration of the lead organizations into an 'Integrated Security Unit' has been successful and should be marked as a significant milestone on the path to enhanced collaboration within Canada's safety and security domains. Despite this, cultural differences also served to degrade the efficiency and effectiveness of the security and safety planning. This was the case across the Policing, Military, and Emergency Management communities. Although there are a number of examples where organizations were able to successfully exploit their differences, such as the Olympic Marine Operations Centre (OMOC) there are also several examples where the gap in organizational cultures served as an impediment and degraded effectiveness and efficiency. The challenges associated with these differences in organizational cultures were prominent in the reporting from the scientific advisors who were embedded within the key organizations. The impact led to delays and inefficiencies as resources were often drawn to nurture relationships and find creative ways to overcome the many differences. Planning doctrine, for example, was not aligned across the primary security and safety delivery agencies. The rigour associated with the Canadian Forces operational planning process, for example, could not be sustained given the degree to which it was misaligned with other security partners planning postures, from which key information was required to advance the planning. In many cases the lack of common doctrine was overcome through the establishment of personal relationships, as reported in a number of After Action Reviews. Literature pertaining to meta-organizational culture will tout the importance of personal relationships; however, not as an alternative to having in place a common doctrine, especially in those domains where it is known that organizations have a longstanding

requirement to work together. The varying degrees of operational planning doctrine and discipline across Departments and Agencies created a significant draw on resources away from the activity of 'planning'. This was also the case with MECSS, where the Scientific Advisors and Project staff was required to work as boundary spanners between the various agencies to overcome these hurdles. It is reasonable to conclude that more research needs to be done to better understand organizational cultures within the security and safety organizations in a domestic context within Canada, and how organizational doctrine might be aligned to bring greater efficiency and effectiveness to multi-departmental planning.

A second component of culture and doctrine pertains to the interface between the security domain and the consequence management domain. The MECSS project team was offered detailed insight into this 'security-safety' interface through the network of scientific advisors who were working across the various domains. Perhaps the challenges associated with the distribution of information between the domains best represent this issue. Understandably, the nature of the security domain calls for strict control of information, especially as it applies to a police investigations or ongoing criminal activity that could lead to a catastrophic event if inappropriately released to the wrong audience. Within the consequence management domain, the doctrine of 'prevent, prepare, respond and recover', most often calls for an open broadcast of information to a wide audience, to accommodate the necessary activities of first responders and the general public in the mitigation and/or prevention of a potential crisis. The sharing of information is further hampered by a consequence management domain that is not well practiced, nor equipped, to manage classified information. The issues associated with the 'security-safety' interface impeded the ability of MECSS to deliver S&T support within both domains. Perhaps the MECSS experience within the CI domain best reflects these challenges, where the bureaucracy associated with the development and approval of a Non-disclosure agreement dramatically delayed S&T activity and reduced the time available to complete the task.

Whole of Government: The complexity of major events safety and security exceeds the capacity of one organization to address all elements. Major Event security requires a comprehensive 'whole of government approach'. Experience from V2010 offers many examples to support this premise. The Olympic national exercise program, which called on a significant degree of S&T support, involved agencies from across all levels of government and jurisdictions. It is a solid example of why a multi-agency approach is necessary. The foundational work conducted by CRTI, which embraces the principles of 'whole of government', was a key element that contributed to the ability of MECSS to deliver support, and is a showcase example of the efficiencies and effectiveness available through a 'whole of government' approach.

Exercises: Although many organizational cultures are not accustomed to being tested or evaluated, the V2010 exercises and the associated planning were the dominant activities in coming to understand the country's capacity and capabilities in terms of safety and security. They were the key events that forced the alignment of capabilities in terms of achieving the intended effect. They were also foundational in terms of legacy resilience for the region, as well as the country. Because of the highly technical nature of many of the exercise scenarios, such as CBRNE, MECSS was able to support the Exercise program through integrated S&T engagement throughout the planning, delivery, and post event analysis. The Exercise program also offered the opportunity for the S&T community to generate and establish its own level of readiness as illustrated by the setup and deployment of Science Town.

Learning: Very few of the security and safety delivery organizations had in place an active process for capturing lessons and maturing these into lessons-learned. As a result, many organizations struggled to learn as they evolved through the planning and operational phases. Processes to capture and transfer new knowledge are not well established within the public security domain. The limited bank of reports from previous major events is testimony to the quality of the existing learning structure. The was recognized by the leadership within the G8/20 Integrated Security Unit, who developed and continue to execute a Knowledge Transfer Plan, with the support of DRDC. There is a strong call from within the RCMP Major Events and Protective Policing directorate for a much more robust lessons-learned process that will bring greater effectiveness and efficiency to the planning for future events. MECSS is supporting the call for learning through the development of a Major Events Security Framework which will guide key partners through the major event planning process, and host a library of reports and tools that were used for previous events.

4.1.2 Set-up

Project Management Framework: MECSS was set up within a project management framework. For the most part, this framework suitably matched the omnibus nature of the activities that MECSS coordinated in the pre-deployment phase of V2010. The pure project management framework did not suit the operational planning elements associated with the deployment of capabilities into an operational environment. The centralized nature and accountabilities of a project management framework conflict with the principles of the operational planning process and deployed operations. As MECSS progressed, it became clear that the operational deployment should have been separated from the Project Management structure from the outset, with a separate line of accountability through DRDC's command hierarchy. Efforts to embed an operational deployment of this magnitude within a project led to unnecessary conflict between the Project leadership and the DRDC Centres' leadership in terms of fiscal accountability and operational planning oversight. Overlaps in accountability led to challenges in establishing consensus in regard to deployment options. In support of the G8/20, the operational planning was separated from the Project management structure, with greater accountability placed on the leadership within the DRDC Centres. With this structure, outcomes were delivered with improved efficiency and effectiveness.

Delivery Model: The MECSS delivery model was dependent upon the project team having a high degree of insight into the challenges facing each of the safety and security delivery organizations. This insight was provided through trusted relationships, which became the centre of gravity for MECSS success. These relationships accommodated an understanding and articulation of the operational requirement as well as the exploitation of the science once it was delivered by the scientific community. The embedded scientific advisors were the key instrument in establishing the level of trust between the organizations, which was supplemented by proactive engagement of the project leadership with the leadership of the security and safety delivery organizations. This experience highlighted the importance of selecting Scientific Advisors with the right experience, skills, knowledge, and interpersonal skills.

4.1.3 Execution

Beyond Authority: Due to the horizontal nature of the MECSS Project, (across several organizations and jurisdictions) many of the project staff were often functioning in a multi-organizational environment beyond organizational authority. This environment can become highly complex and calls on unique skills and knowledge that are not typically nurtured within individual Departmental career progression. Understanding this environment and learning the skills to function within it will become an increasingly significant factor for the S&T community as it evolves deeper into public security and the 'whole of government' domain.

Leadership Engagement: The MECSS Project was set up to support the functional authorities in reducing the security risk associated with V2010. When MECSS began providing support, the functional authorities were already engaged in an operational rhythm to support the pace of decision-making that was essential for the security posture to be in place in time for V2010. To demonstrate value-added, MECSS had to establish a decision-loop which accommodated the operational tempo. Direct access to DRDC leadership played a key role in the Project's ability to deliver support. During the planning, the MECSS Project Leader was engaged with the ADM (S&T) on an almost daily basis, where updates were provided and decisions taken. During the operational deployment, ADM(S&T) was briefed on a daily basis by the DRDC Ops team which included MECSS Ops, DRDC PA, and CO Military Support Unit. As well, the ADM delivered decision-making authority to the Project Leader (through the DRDC Operational Directive) in the event he was not available and an urgent decision was required. MECSS also received complete support from the leadership with the DRDC Centres, which was apparent on several occasions, especially those associated with last-minute unforecast calls for resources.

Governance: Engagement by the key security partners through a Senior Review Board governance structure, within the Public Security Technical Program, was an important element in establishing a trusted relationship with the leadership in the security delivery organizations, as well as the science community. The SRB permitted each representative an opportunity to influence the investment priorities of the Project. This legitimized the objectives of the Project from the perspective of the other agencies

4.1.4 Legacy

There are several legacy outcomes from the MECSS Project. These can be considered within the context of: Institutionalized Science and Technology, New Capabilities, and Knowledge Transfer. Figure 4 illustrates the primary legacy outcomes from the S&T support to the Olympics, the G8, and the G20.

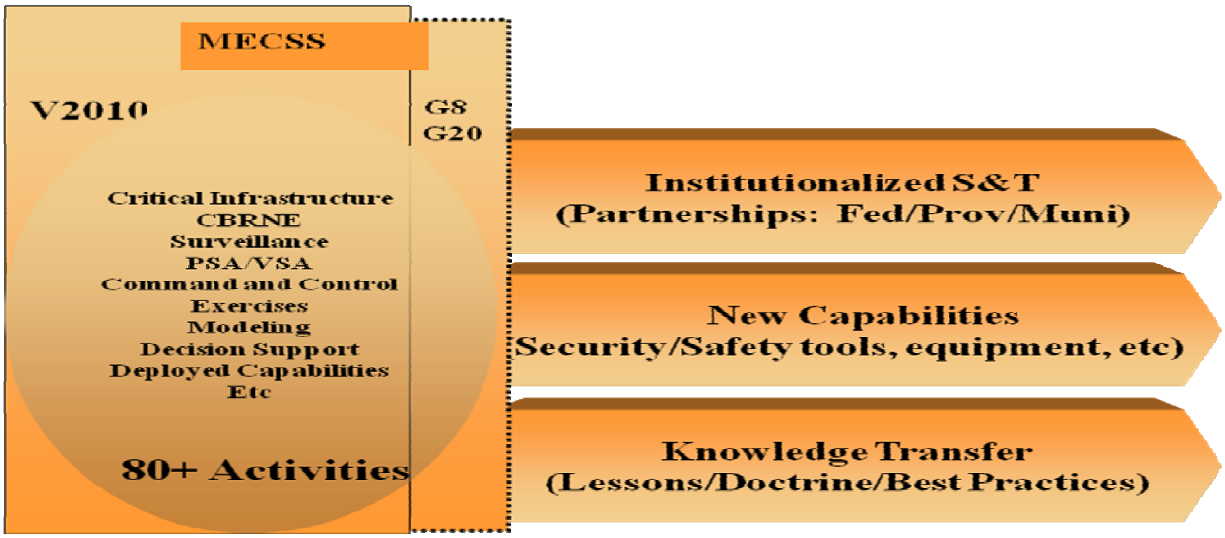

Figure 4: MECSS Legacy

Institutionalized S&T: This refers to the degree to which S&T has become embedded within the practices of various organizations. As an outcome from MECSS, S&T is now embedded in organizations that previously did not have access to S&T support through DRDC. For example, the RCMP Major Events and Protective Policing Directorate and DRDC CSS have formalized a relationship that will provide an embedded scientific advisor within the RCMP for the foreseeable future. As well, the Province of British Columbia has requested long-term support from DRDC, which is being managed through a formal agreement. As well, international partners have taken notice of the degree to which Canada used S&T to enable security capabilities. Collaboration with the UK, for example, is ongoing in support the London Summer Games. These are examples of how S&T is being institutionalized within the security and safety partners.

New Capabilities: V2010, the G8, and the G20 served as a forcing function that pushed the development of capabilities to meet operational needs. MECSS served as a vehicle to advance new technologies. The best example is Science Town. During the period leading up to the Olympics, new mobile laboratories for Chem, Bio, Rad, and Forensics were delivered and integrated into a capability the delivered real support during critical, high profile operations.

Knowledge Transfer: One of the chief concerns raised by a number of operators during the course of the planning was that the new knowledge gained over the years of preparations would be lost. The knowledge transfer component of the MECSS legacy attempts to mitigate a portion of these concerns. During the life of the project, over 200 scientist and technicians were engaged, leading to the publishing of approximately one hundred and sixty scientific, peer-reviewed reports. These Reports reflect the support that was provided during the planning, exercises, as well as operations. Some Reports have already been called on to support G8 and G20 planning. The MECSS experience allowed for the collection of data that will be used as the foundation for future reports. For the G8 and G20, the Integrated Security Unit called on DRDC to support their Knowledge Transfer Plan. This work will continue into 2011and have significant benefit to future security operations associated with Major Events. The After Event Report (AER) was written for Privy Council Office and is an off-shoot of MECSS support to the PCO Office of the Coordinator of Security for the Olympics and G8. This report was prepared for the National

Security Advisor and brings strong scientific rigour to the analysis of key safety and security issues that were identified from a 'whole of government' perspective during V2010 planning and operations. The most significant element of MECSS that supports the transfer of knowledge to future planning teams is the Major Events Security Framework. This forum institutionalizes a multi-agency planning process for Major Events, which will provide immediate access to the bank of plans, reports and tools that have been used for other security events.

4.2 Project Manager's Observations

The Project Team was directed to manage support to the V2010 Olympics and Paralympics using a project framework similar to that used by Technology Demonstration Projects. This framework provided sufficient governance and accountability and was very familiar to the DRDC Centres however had not been previously applied to public security Project. This resulted in an organizational learning curve as the requirements of project management needed to be adjusted to the flexibility needed for the public security community. The Synopsis Sheet proved to be a valuable tool to control scope, confirm project authority and was referred to frequently as the project progressed. The project framework was a less-than-optimal structure for dealing with the planning of the actual deployment of DRDC resources during V2010 as it lacked the flexibility and responsiveness needed to respond to last minute requirements and changes. It would have been preferred to have a dedicated operations staff planning the deployment using the operational planning process.

During the initiation phase of the project, a number of scientific domains were identified to help structure the work. While it was difficult to predict the areas that would require the greatest effort from MECSS it was felt that the identified domains covered the majority of areas where MECSS would be capable of contributing. The only domain that was identified and did not progress as planned was Psycho-Social. This was not due to lack of interest, but rather due to the lack of a Domain Lead that could be readily engaged and to a clearly identified client that would benefit from the work done. As the project progressed, a number of areas of work were difficult to tag to a specific domain (eg VSA/PSA and Cyber). The project team would have benefited from revisiting the domains part way through the project.

Domain leads were a great match. Those that agreed to lead domains had a great depth of knowledge and a broad understanding of the work done in the area the capabilities available both within DRDC and the federal S&T community. Initially, there was some uncertainty as to the scope of responsibilities of the domain lead, however each one embraced their areas and quickly gained credibility with the primarily clients. Their involvement was critical to ensuring quality S&T was delivered. With the exception of Surveillance (changed once), the domain leads remained throughout the project allowing for continuity of effort.

The use of Scientific Advisors (SAs) co-located with the partners was one of the best decisions in the project. The degree to which the SAs were integrated varied with each organization, however each one brought a great deal of expertise to bear and generated trusting relationships with the partners. Their position close to the decision-makers allowed them to adequately introduce opportunities to exploit S&T. This concept was so successful that Scientific Advisors will remain within the RCMP and the Public Safety Canada Government Operations Centre beyond MECSS.

The selection of Scientific Advisors was done both competitively and non-competitively - both methods worked well to select the most appropriate persons for the tasks. Deploying the SAs to Vancouver proved to be especially challenging due to the lack of administrative support in the area and within CSS. The decision was made to deploy the SAs on travel status instead of relocating them primarily due to the cost of housing in the Vancouver area and the need to attract individuals to the assignment in a short period of time. This option was at a significantly higher cost and introduced much ongoing conflict in the interpretation of the Treasury Board Travel Directive but was still necessary to ensure quality candidates would be interested.

Funding for MECSS was provided from the Agility Fund and CRTI. The project was sufficiently funded for the work that was conducted and the agility fund was a flexible mechanism. The provision of a centralized budget provided the flexibility for MECSS to respond to requirements as they arose. In the absence of centralized funding for domestic operations, most of the Centres would be unable to contribute as they did. CRTI funding was not provided during the first year of the project and once provided, was used to deliver the portions of the MECSS project dealing with CBRNE and the Framework. Costs related to the deployment of DRDC personnel was covered by Agility Funds.

The over-riding consideration to accept work was whether or not we had access to federal expertise that could be exploited and provide value-added (as opposed to just hiring contractors). Where expertise was not accessible in-house, the work was not undertaken. In cases, where DRDC expertise existed to deliver, this was the preferred option although in some situations contractors were used to assist the DRDC personnel. The quality of work provided by the DRDC teams was significantly higher than that provided by contractors.

The contracting process was not a significant impediment to the delivery of MECSS. Because of the short timelines, contractors were only considered in circumstances where existing contracts were already in place. In particular, MECSS was able to make use of the Supply Arrangements and the Integrator contract set up for the JCDS 21 project as well as a CBRNE contract held by Director General Nuclear Safety (DGNS).

The MECSS project engaged S&T resources from each of the DRDC Centres as well as many of the federal S&T organizations. This proved to be a challenge as each organization had its own administrative procedures for dealing with travel, overtime and contracting. Overtime proved to be especially controversial as the interpretation of the collective agreements differed between Centres resulting in unequal compensation within the same working team for similar work. In particular, the handling of overtime for the deployment period was left to each Centre to resolve with the result that three different approaches were used. The different interpretations of policies created conflict within the project but highlighted the need for centralized guidance to create a consistent and fair interpretation for DRDC employees.

From the outset, MECSS had planned for a reactive communications posture primarily because of the operational context under which the work was conducted. This posture led to a revised publication process that used the CSS Document Review Panel to avoid unnecessary exposure of operationally sensitive information. This revised process was cumbersome and insufficiently resourced within the MECSS project resulting in many unacceptable delays. The majority of deliverables from MECSS were letter reports that did not require extensive staffing or review. In most cases, draft versions were provided to the partners pending official release. The draft

versions were sufficient to support the decision-makers. One issue that continues is to track down all of the reports that were provided. Some information was provided by PowerPoint and copies were not always forwarded to MECSS.

The MECSS team was very decentralized and dependent on distributed tools such as teleconference, videoteleconference, the DRDC SharePoint portal. The progressive exploitation of these tools greatly enhanced internal communications amongst the team, and served as an effective tool for capturing records of activity. Towards the end of the project, we discovered that backups were not being properly done resulting in a loss of some of the data

4.3 Exploitation Officer's Observations

This segment will provide an overview of the Exploitation role within the MECSS Project and the challenges experienced in regards to level of engagement and cultural differences between the founding project partners. Additionally, successes from the main domains of work undertaken as part of MECSS will be outlined as well as recommendations for potential exploitation opportunities.

It is crucial first to understand the goals of project exploitation and how results of work done as part of the MECSS Project to support Major Events security and the V2010 Games security operation. "Exploitation" refers to the act of employing something to the greatest possible advantage for the individual or organization. In terms of results of a project such as MECSS, where numerous security related domains were studied, it is clear that benefits will be realized by RCMP Protective Policing in regards to major events security operational processes for the future. Potential benefits however, are certainly not limited to this area. There are many sectors within the RCMP as well as in partner organizations both domestic and foreign that can utilize MECSS deliverables to their advantage. By engaging these sectors, the results of MECSS can be multiplied and further development opportunities explored.

4.3.1 Exploitation Opportunities

The MECSS Project provided comprehensive S&T based support to the RCMP-led security planning and operations for the Vancouver 2010 Olympic and Paralympic Games, and in support of G8 and G20 Summits security planning. MECSS also included the development of an enduring security framework for future major events operations, an aspect that is continuing. Exploitation opportunities identified for each relevant domain of study are as follows

a. Major Events Security Framework

RCMP Protective Policing

- Developed as part of the MECSS Project, the purpose of the MESF is to provide RCMP organizers of Major Event security operations with a basic framework that should be followed for planning their participation in a Major Event in Canada. This framework will assist planners and project managers in the construction of organizational structures, lines of command and control and with the definition of specific roles and responsibilities.

- The MESF is the key legacy piece for the RCMP from the MECSS Project. It will be used as the standard by which RCMP planning is done for all future major events security operations. It will also incorporate federal partner departments and ensure a truly integrated and collaborative approach to major events security planning

b. Psycho-Social Domain: State of Science Report

G8/G20 ISU - Public Affairs Communications Team (PACT) and Community Relations Group (CRG)

- The G8/G20 Integrated Security Unit (ISU) was responsible for the planning and implementation of security for the G8 and G20 Summits.
- This report was provided to the G8/G20 PACT and CRG for their consideration during the planning phase for the Summits, with positive feedback received regarding the value of the information provided.

RCMP Protective Policing – Major Events Security Framework

- This work will be incorporated into the MESF as a reference document.

RCMP National Communication Services (NCS)

- National Communication Services is the national policy centre for all RCMP communication. NCS is responsible for providing advice and support to operations, business lines, regions and divisions on communication matters.
- NCS have been provided a copy of the work done in this domain and have expressed an interest in being included in the dissemination of future related studies.

c. VSA/PSA Analysis: Human Factors Report

RCMP Protective Policing – Major Events Security Framework

- This information will be included as a reference document within the MESF.

RCMP Occupational Health & Safety

- The RCMP is by far the largest police force in Canada and employs a large workforce of extremely diversified occupations. The bulk of this workforce is composed of Police Officers in the more traditional way, but also includes a wide variety of specialized officers and Civilian members and public servants, auxiliary constables, volunteers and contractors from all trades and professions. This creates a situation almost unique to the RCMP where it becomes necessary to deal with very diversified environments and risks, scattered across the country. The RCMP requires a range of measures exceeding the scope of occupational safety found within most other federal departments. OH&S has its main goals to support and promote the establishment of a safe work environment and safe work practices and to reduce the frequency and severity of work-related accidents, incidents, injuries, illnesses.

- This focused look at employee safety and impacts that workplace conditions have on security personnel working VSA/PSA duties will be shared with OH&S to be used as a planning reference for future related policing activities.

RCMP CAP - Operational Policy & Compliance

- Policy and Compliance Section initiates, co-ordinates and is responsible for policy in the Operational Manual that directly impacts police operations. This section reviews issues and concerns from field personnel and acts as a resource for other policy centres.
- The Human Factors report will be shared with the Operational Policy & Compliance Section and will be valuable for policy revision and development in terms of operational procedures.

UK: London Metropolitan Police – 2012 Olympic Security Planning

- A comprehensive knowledge transfer process is under way to assist the UK security planners for the 2012 Games by sharing lessons learned and best practices garnered from the V2010 experience. The UK has expressed an interest in the work done in this domain and consultations with MECSS representatives are under way.

e. VSA/PSA Analysis: Dooley Reports

RCMP Protective Policing – Major Events Security Framework

- This information will be included as a reference document within the MESF.

RCMP Property Security Section

- The Property Security Unit (PSU) provides the accommodations security for all of RCMP facilities within the National Capital Region (NCR).
- The range of duties includes the access and egress control at all major RCMP facilities, continuous patrolling of all sites, fire orders, the provision of building security badges and the administration, assignment and enforcement of parking.
- VSA/PSA reports are of potential use to PSU, particularly in the event that enhanced vehicle and pedestrian screening needs to be put in place as a result of elevated threats to RCMP facilities. PSU has expressed an interest in having access to these reports.

CATSA

- The Canadian Air Transport Security Authority (CATSA) is a Crown corporation charged with protecting the public through effective and efficient screening of air travelers and their baggage.
- Information obtained during MECSS could be of great interest to CATSA; opportunities for sharing the analyses will be explored.

UK: London Metropolitan Police – 2012 Olympic Security Planning

- A comprehensive knowledge transfer process is under way to assist the UK security planners for the 2012 Games by sharing lessons learned and best practices garnered from the V2010 experience. The UK has expressed an interest in the work done in this domain and consultations with MECSS representatives are under way.

f. CBRNE Domain: Science Town, Capability Analysis for Province of BC

RCMP Protective Policing – Major Events Security Framework

- This information will be included as a reference document within the MESF.

National CBRNE Response Team

- Led by the RCMP, this multi-agency team is responsible to respond to CBRNE incidents occurring anywhere in Canada.
- The concept for, design of and deployment of expertise in the form of a science town at significant major events has been shared with the N CBRNE RT.
- Understanding existing capacity is vital in ensuring adequate response to CBRNE incidents. Although the information obtained in this analysis will no doubt be out of date in relatively short time frame, it remains useful, particularly in the capture of the methodology used to evaluate capacity gaps.

Further Development Potential: Similar analysis for each Province/Territory; Strategy to maintain information (ever-greening)

g. CBRNE Domain: Exercise Live Play (Scenarios & Injects)

RCMP ORR – National Exercise Program

- The RCMP conducts regular exercises both independently to challenge internal procedures and to ensure that the RCMP, working with partners, is prepared to mount a coordinated and effective response to incidents of all kinds. The RCMP National Exercise Program provides expert advice, guidance and coordination to exercise activities across the organization.
- The scenarios and injects specifically developed in terms of the CBRNE can be used for future exercise activities.

RCMP Protective Policing – Major Events Security Framework

- This information will be included as reference documents within the MESF.

h. CBRNE Domain: Clandestine Lab Training Facility

Vancouver Fire Department

Vancouver Police Department

Other BC First responders' training units

i. Critical Infrastructure Domain: I2Sim, Interdependency Models, Blast Analysis

Public Safety Canada

- PS Canada develops national policy, response systems and standards in regards to critical infrastructure. PS Canada's National Strategy and Action Plan for Critical Infrastructure establishes a risk-based approach for strengthening the resiliency of Canada's vital assets and systems such as the food supply, electricity grids, transportation, communications and public safety systems.
- There is obvious potential for the work done in this domain to be of use to PSC. The possibility of sharing reports with them will be explored.

Province of BC (EMBC)

- The Provincial Emergency Program (PEP) is a division of the Ministry of Public Safety and Solicitor General, Emergency Management BC. PEP enhances public safety and reduces property and economic loss from actual or imminent emergencies or disaster by providing leadership, expertise and resources towards promoting individual and community awareness and preparedness; advising the Province, local authorities and First Nations on emergency prevention strategies; coordinating and ensuring timely responses to emergencies and disasters; and collaborating with agencies to provide for coordinated recovery and reconstruction efforts.

RCMP CIP – Critical Infrastructure Criminal Intelligence (CICI)

- The critical objective of the Criminal Intelligence Program (CIP) is to enable sustainable organizational intelligence-led policing. This program enhances the RCMP's ability to protect Canadians from current or emerging criminal trends by providing the tactical and strategic criminal intelligence necessary to guide operations. Part of CIP, CICI focuses on critical infrastructure, threats surrounding it and impacts associated with failure or attack of CI assets.
- The I2Sim methodology is of interest to CICI and the possibility of sharing knowledge garnered through MECSS in the use of this system will be explored.
- Interdependencies of CI assets in the Greater Vancouver Area identified during the MECSS Project are relevant to the mandate of CICI. The possibility of sharing information obtained with CICI will be explored.

Vancouver Police Department

- As the police force of jurisdiction in the city of Vancouver, information regarding the security of critical infrastructure in the Greater Vancouver Area is of interest to VPD.

RCMP ORR – Geospatial Intelligence Section

- This section provides a digital mapping service which uses Geospatial Information Systems (GIS) technology. It provides operational support to internal clients such as Major Events, Criminal Intelligence Directorate (CID)

and Integrated Border Enforcement Teams (IBET). It also manages a mapping data library which can be shared with any RCMP section to support their operations. One area for which they use the data is in conductung blast analyses in evaluating potential threats posed by explosive devices in and around secure sites.

- The blast analysis work done as part of the MECSS Project will be shared with RCMP ORR for their information and as future reference. Additionally, the methodology of the analysis could be made available to them

j. Surveillance Domain: Marine Threats

RCMP Protective Policing – Major Events Security Framework

- This information will be included as reference documents within the MESF.

G8/G20 ISU - Marine Planning

- The G8 and G20 Summits, held in Huntsville and Toronto respectively, each had water-side security concerns. The information obtained as part of the work done pre-Olympics was of use to the ISU planners during preparations for the Summits.

RCMP Federal & International Operations – Marine & Ports

- The goal of the Marine and Ports Branch is to prevent, deter and detect illegal activity, such as cargo or people who may pose a threat to the safety and security of the marine environment in Canada, the United States and the international community. The Marine and Ports strategy is based on an integrated approach that focuses on reducing the vulnerabilities of our marine systems and facilities, with respect to terrorism and organized crime.
- The information obtained through the MECSS activities in regards to marine threats is of great interest to the M&P Branch and will be provided to them for future reference.

CF

- In the context of Major Events, the CF will continue to work with the RCMP and would benefit from joint technologies and concepts of operations

k. Exercises Domain: Methods (General Paper), Force Protection Matrix Game

RCMP ORR – National Exercise Program

- The RCMP conducts regular exercises both independently to challenge internal procedures and to ensure that the RCMP, working with partners, is prepared to mount a coordinated and effective response to incidents of all kinds. The RCMP National Exercise Program provides expert advice, guidance and coordination to exercise activities across the organization.

- The paper will be a valuable reference for the National Exercise Program in improving exercise design and execution.

G8/G20 ISU – Exercise Planning

- G8/G20 exercises benefited greatly from the work done in this domain during the MECSS Project. Methodology and lessons learned assisted the Summits exercise planners prepare and carry out tests from the basic unit level to multi-sector organizational exercises.

RCMP Protective Policing – Major Events Security Framework

- This information will be included as reference documents within the MESF.

l. Command & Control Domain: Business Modelling, Command Centre Design, Handover Strategies

RCMP Protective Policing – Major Events Security Framework

- This information will be included as reference documents within the MESF.

G8/G20 ISU – UCC & C2 Planning

- The G8/G20 ISU used the information resulting from the MECSS work in this domain to assist in the design and construction of the Unified Command Centre in Barrie.
- The ISU stood up several command centres to manage operations during the Summits. Handover strategies were shared with the ISU and were very valuable in developing C2 plans in each of the command centres.

RCMP ORR – National Operations Centre (NOC)

- NOC is the principal contact point between the RCMP and key national and international crisis and emergency partners. It is responsible for the continued relationship and enhancement of multi-departmental working groups involved in national security and counter-terrorist plans. The centre implements the newest technologies to enhance national and international co-operation in the communication of time sensitive sharing of tactical and strategic information and intelligence. It includes a command centre from which significant events and operations, both domestic and foreign, are monitored and managed from an organizational perspective.
- NOC will be relocated to the new RCMP HQ in Ottawa south and is in the process of modernizing its design prior to construction. The design work done in the course of the MECSS Project has been shared with the planners and will prove very valuable in the development of the new NOC design.
- The efficiency of information transfer as shifts are changed within the NOC can be enhanced using handover strategies developed during the MECSS Project.

m. Command & Control Domain: SA Tools

CF

4.3.2 RCMP Engagement

Initially, the vision for the level of RCMP engagement in the project team was committed to the provision of a full time exploitation officer from the Major Events and Protective Services (ME&PS) Branch, to be embedded in the project office. Unfortunately, the priorities and pressures associated with upcoming significant major events in 2010 negated the possibility of the Exploitation Officer being dedicated full time on MECSS. Early in the project, the Exploitation Officer was assigned to the position of Federal Security Coordinator for the V2010 security operation and as such, the majority of this officer's time was dedicated to this function, with MECSS activities being given lower priority. This resulted in a disconnect at the strategic level of the Project, with the ME&PS sector of the Force not being as engaged as envisioned and as would have been ideal. It is recommended that should the RCMP decide to become involved in future projects of this nature, a commitment to the provision of a full-time, dedicated RCMP project lead should be made.

4.3.3 Cultural Challenges: RCMP and DRDC

One of the main challenges experienced during this project was in encouraging collaboration between two organizations with significantly different cultures. Despite the fact that each organization was focused on the same basic goal (i.e. ensuring a secure Olympic Games in Vancouver), there seemed, at least initially, to be an inherent mistrust and a general lack of understanding between the RCMP and DRDC. While there was obvious buy-in from senior ranks of the RCMP at the HQ level for this project, the V2010 ISU was hesitant to include the DRDC Scientific Advisor in their planning unit. There was a lack of understanding on the part of RCMP planners as to the role of DRDC CSS and its reason for offering such generous and unsolicited support to an RCMP-mandated activity. DRDC was widely looked on as strictly part of DND and CSS' wider mandate to provide security-related S&T support across all federal departments was not common knowledge.

Once DRDC's Scientific Advisor was on site at the V2010 ISU, planners began to recognize the value of the support being offered and, over time, they became more willing to engage DRDC in seeking S&T solutions when planning issues arose. That's not to say that there were no further challenges. Police planners are very protective over sensitive planning information and, as such, there were concerns that DRDC would not adequately restrict information dissemination of operational material. DRDC mitigated these concerns by ensuring all reports with even marginal potential to be considered sensitive by their RCMP colleagues were classified at minimum a Protected B level. Their strict adherence to the classification of documents went a long way in assuaging RCMP concerns in this regard.

The cultural challenges encountered were not, of course, strictly one-sided. MECSS personnel often displayed a lack of understanding for the realities of ongoing operational priorities of the RCMP. One particular example is in the criticism by some MECSS personnel of the RCMP for not ensuring all V2010 operational commanders were present throughout the major exercises (Bronze, Silver Gold). While the RCMP recognized that it would have been ideal to have these officers on site throughout the extensive exercise periods, the reality was that these individuals

were fully engaged in day-to-day police operations in their respective home units. It would have been tactically imprudent to pull them all away from ongoing responsibilities at the same time for a non-operational reason. It is not difficult to understand where the differences in cultures caused this particular disagreement. Generally when in Canada, CF personnel are not in an operational role and can be entirely dedicated to training and exercise activities. The RCMP does not have that luxury and training and exercise activities must be balanced with day to day police operational needs across the country.

It is difficult to solve these kinds of issues in a short time frame however there are lessons we can learn from the experience. Future collaborations should be preceded by a comprehensive education piece. RCMP members, from the working level right up to the event commanders, should be made aware of the mandate of CSS, DRDC and how support of major event security activities falls within their mandate. Likewise, DRDC personnel would need an orientation in regards to RCMP major events security planning and the inherent challenges to normal operations both during the planning phase and execution. Both organizations would benefit greatly from some sort of familiarization with the other and all employees must be encouraged to seek to understand the actions of their counterparts, rather than rushing to criticize them.

4.4 Comments on Project Assumptions, Constraints and Risk Factors

4.4.1 Assumptions

All of the assumptions identified in the Synopsis Sheet provided to be valid with the exception of one. The assumption was that the RCMP would be able to take over the results of the MECSS project and exploit them further. In the end, there was insufficient capacity for the RCMP to take over all the results. They have taken control of the Major Events Security Framework, but the remainder are still under DRDC control.

4.4.2 Constraints

The only constraint put on the project that did not materialize was the expectation that much of the work would need to be done at the Secret level. In the end there was limited requirement for classified communications capability. Most of the work was done at the Protected B level for the RCMP, unclassified for the province with limited work at the Secret level for the CF.

4.4.3 Risks

Although initial planning identified a number of risks, little time was spent systematically reviewing the risk management plan. The following Risks were identified:

a. Time. This project had a fixed end date which meant delays of deliverables were not acceptable. The impact of this risk meant that some tasks could not be started or were terminated early because of the tight timelines.

b. Expectations. This risk was identified to address the expectations of the clients. This was less a problem than the expectations of the scientific team that they would have the time and latitude to apply full scientific rigour. In nearly all cases, the operational clients were more than satisfied with best effort from the MECSS team.

c. Science maturity. This proved to not be a major issue as the stakeholders were only interested in S&T at high level of technical readiness.

d. Impact on RTA. At the beginning of the project, there was concern that the pull of resources for MECSS might have a negative impact on the RTA program. Feedback from the Centres has indicated that this is not the case. It should be noted that MECSS used significant resources from Suffield, Toronto, CORA and CSS.

e. Lack of governance. This became an issue for Science Town discussing reporting mechanisms during V2010. The pre-existing relationships from CRTI clusters helped create a positive working environment and a spirit of cooperation.

f. Contract award delays. The mitigation strategy was used with great success. The JCDS 21 contract and the ISR contracts were made available on a priority basis for MECSS and were invaluable. Without pre-existing contracts, we would not have been able to meet the short timelines.

g. Accommodations. The mitigation plan involved keeping people close but not right in the city. This was not possible because co-location with the partners was required. In the end, accommodation was found for all employees in the vicinity through RCMP/PWGSC standing offers, but at a very high cost.

h. Security classification. All MECSS employees were able to work at the Protected B level using the DWAN and PKI card. In order to communicate with clients, the Scientific Advisors were able to air gap the reports and information. Access to TITAN for Secret communications was not provided at CSS until after V2010, therefore all operations work at that level was done at 305 Rideau.

i. One key risk that was completely missed in planning was the risk that the DRDC Network would become unavailable during the operation. This risk did not materialize during V2010; however technical issues were encountered between V2010 and the G8/G20. This meant that the primary communications means was formally moved to the DND Network for G8/G20 however not all of DRDC was able to communicate using this means, especially remotely. A more effective contingency plan is needed for future domestic operations.

4.5 After Action Review

4.5.1 Best Practices

The MECSS project achieved the greatest value from embedding Scientific Advisors with the stakeholders. This allowed them to become integrated into their decision cycles. In many cases,

the partners did not understand where and when S&T could help them. A Scientific Advisor co-located allowed them to informally explore options without committing to certain actions or extensive resources. The Scientific Advisors for MECSS had extensive organizational experience and were very aware of the expertise available and the limitations to that expertise. With time, the Scientific Advisors were able to generate trust with the stakeholders that increased the extent to which they were consulted as well as the adoption of recommendations. Attempts to provide Scientific Advisors that were not co-located had limited value as they were not visible and therefore not considered. There are numerous examples where scientific advisors influenced planning by providing quick reach-back to appropriate expertise in DRDC.

MECSS used a combination of contractors and employees to deliver S&T results. The greatest value was obtained from using employees over contractors. Public servants are well positioned to respond quickly to operational needs whereas contract resources resulted in significant delays putting contract tasks in place, even in the circumstances where contracts were already in place. In addition, public servants have a better understanding of the operational context through multiple years of experience with the organizations while contractors take time to develop this knowledge. In addition, the knowledge generated from completing the work has a legacy value with employees and can be re-accessed easily whereas contractors take their enhanced knowledge with them at the end of the task. The quality of the work performed by the public servants in MECSS was far better than that delivered by the contractors.

The MECSS project was able to develop a great working relationship at the tactical level. This included staff officers from the military, RCMP and province that had responsibility for operational delivery. This is where operational S&T has the greatest payback.

Tactical engagement of the project team was only made possible due to early stakeholder engagement at the strategic level during project initiation. This ensured maximum support for the planned activities at the highest level and this support was communicated to the staff offers. …

During V2010, the operational deployment of DRDC personnel and equipment was managed in the context of a project activity. This was not the preferred way and the problems encountered during V2010 were avoided during the G8/G20 by separating the DRDC Deployment planning from the Project activity, and assigning greater accountability to the leadership within those DRDC Centres that would be deploying personnel and/or equipment. Planning and execution of an operational deployment of S&T is too dynamic to fit with a formal project construct, therefore any such element requires dedicated staff officer support.

One particular problem encountered during V2010 was the extent to which logistical support was centralized by MECSS. This approach was necessary and unavoidable for V2010 because of centralized funding and accommodation contracts as well as the expected high expenditures. Due to insufficient staff and lack of common DRDC procedures, this created conflict with numerous unresolved issues. For the G8/G20, logistic support related to the deployment of S&T workers was handled by the Centres. While funding for overtime and travel still needed to be negotiated with MECSS, the Centres did an excellent job looking after the logistic needs of their employees. Funding for future deployments will still need to be resolved, but the Centres are still in the best position to handle all of their own employee logistic needs

4.5.2 Challenges

The federal government has a clear security and information management policy however the province of BC does not have comparable security classifications. Not only did employees not have security clearances, but no guidelines for the handling of sensitive information exists that could equate to the federal directives. This made creating and sharing information with the provincial stakeholders a challenge. In most cases, the resulting work needed to be unclassified. An example of this would be the deficiencies noted during CBRNE training and exercises. In order to enable improvement, the results needed to be unclassified even if there was a risk.

One of the roles of MECSS was to provide reach-back into DRDC for additional expertise. This was a challenge for MECSS because there is no knowledge base of DRDC expertise and where it exists. The MECSS team was forced to resort to informal networks to reach those who could help.

The MECSS project did not have a knowledge manager until very late in the project. This meant that we were not well positioned to capture and integrate lessons learned from the beginning. In addition, the MECSS team greatly underestimated the number of reports that would be delivered and the short time frame in which they would be required. MECSS had insufficient resources to receive, review, accept and distribute the results. This meant delays getting reports to the stakeholders and in the end, draft versions were delivered to enable decision-making.

MECSS took on a passive Communications Plan in terms of delivering information to outside agencies or the public. Initially, it was identified that the best way to protect our fragile relationship with the security partners was to minimize all external communications that could in turn be perceived as threatening to the policing community. As a consequence, opportunities to showcase DRDC support and garner support for future public security programs was marginalized or lost.

Despite multiple attempts to generate an exploitation strategy, the MECSS project was challenged to ensure sufficient resources were available and in-place to support post-MECSS activity. Much of the MECSS legacy activity does not fall naturally within the scope of the three programs managed within DRDC CSS; therefore the MECSS PD and PM had to be creative in finding a champion and suitable resources to support follow-on activity. In some cases, these were not found, and it is expected that the activity will flounder until the work is appropriately prioritized and resources are assigned.

A significant challenge for the MECSS team was the need to understand the organizational culture of the policing and emergency management communities. Many DRDC employees did not fully understand the RCMP culture and initially approached the work with the same mind-set as they would for a military client. Initially, DRDC support was seen as ‘military’ support which appeared to make the advice difficult for some groups to accept. In the same way, the partners did not completely understand the S&T capabilities and how they could benefit planning

4.5.3 Recommendations

MECSS had a great impact and in the end was well received by the partners for both V2010 and the G8/G20. It is expected that demands for similar work in support of domestic security

operations will only increase. The following recommendations are made to support future S&T support to domestic safety and security planning and operations:

a. Many of the activities conducted through MECSS were non-traditional for DRDC. Despite this, DRDC played a strong leadership role in operationalizing national S&T capacity in support of domestic public security operations. Without MECSS, the infrastructure is no longer in place to effectively support ongoing planning, exercising and operations for other key public security events. It is recommended that DRDC formalize and appropriately resource a program to provide ongoing support to public security planning and operations in Canada.

b. It takes time to build trust with external organizations. It is recommended that scientific advisors should be embedded with the planning teams early to contribute to decisions support;

c. A lack of appreciation of different cultures can not only delay acceptance, but could result in rejection of advice or the provision of unsuitable advice. It is recommended that further research be conducted in regard to organizational cultures within Canada's safety and security domains, and that this research serve as the foundation for organizational culture sensitivity training for those deploying in direct support of the public security partners.

d. The staffing process to task DRDC Centres was created for MECSS. The requirement to task Centres for future operations remains. It is recommended that DRDC develop a more rigorous staffing process to accommodate formal direction from the ADM (S&T) office to the DRDC Centres in terms of tasking resources to support operations.

e. Sufficient admin support is needed for a project of this scope. As a minimum, the project requires a dedicated admin assistant to manage travel and official files, a knowledge manager to handle report generation and a finance clerk to handle contracts, invoices and funds transfers.

The concept of Science Town proved to be a valuable one and work needs to continue to develop and test the concept. Issues to be resolved include the validation of mandates and the availability of sufficient resources to ensure sustainability of the capability.

5 MECSS Reports

Fact Sheets for C2 Demo Day Held at StarTop Road, 24 Oct 2008 (2008).

Allen, D. (2009). *Comparison of Planned and Observed Processes for Major Event Security - Results from Pegasus Guardian 1* (Technical Note).

Allen, D. (2009). *Modeling Information Management Processes for Major Event Security* (Technical Report).

Allen, D., Bélanger, M., & Goodman, L. (2010). *Feedback on the ISU 2010 Summits Command and Control Document Version 0.3* (Letter Report - PA).

Allen, D., Breton, R., & Hancock, J. (2009). *Initial Analysis of ISU Whistler Area Command Centre (WACC) Operations during Exercises Pegasus Guardian 3 and Gold* (Letter Report - PB).

Allen, D., Farrell, P., Chow, R., & Trinh, K. (2009). *Pegasus Guardian Experiment Analysis Report* (Technical Report).

Allen, D., Maceda, E., Smith, D., Wood, D., Gouin, D., Jobidon, M.-E., et al. (2009). *Initial Analysis of ISU Vancouver Area Command Centre (VACC) Operations During Exercises Pegasus Guardian 2-2 and Silver* (Letter Report - PB).

Baingo, D. (2010). *Blast Effects Analysis in Support of Security Operations for the Vancouver 2010 Winter Olympic Games* (DRAFT Technical Report).

Baingo, D., & Chouinard, P. (2008). *Briefing Note to the ISU on Interim Analysis of Games Related CI Assets* (Letter Report - S).

Baker, K., & Hales, D. (2008). *V2010 Command and Control Architecture - Initial Data Collection at the Integrated Security Unit* (Contractor Report).

Baker, K., & Hales, D. (2010). *Vancouver 2010 Command and Control Architecture: Initial Needs Analysis* (Contractor Report - PB).

Beaudoin, L., & Genik, L. (2009). *Cyber Incident Communication Structure* (Power Point Presentation).

Beaudoin, L., & Genik, L. (2010). *Review and Coordination of Cyber Security for Vancouver 2010*. Paper presented at the Knowledge Systems for Coalition Operations 2010

Beaudoin, L., & Genik, L. (2010). *Vancouver 2010 Key Cyber Stakeholders* (Power Point Presentation).

Beaudoin, L., Scheurkogel, N., & Genik, L. (2010). *Vancouver 2010 Cyber Security Review* (Letter Report).

Bélanger, M., Sahi, A., & Guitouni, A. (2008). *Synthesis: Lessons Learned From CIS Deployments* (PowerPoint Presentation - S).

Billyard, A. P., & Collin, I. A. (2008). *Vancouver 2010 Olympics: Identifying CF Communication Issues Associated with the CH-146 Acting as Interceptor (not yet received)* (Technical Memorandum - S(CEO)).

Boury-Brisset, A.-C., Dessureault, D., Gagnon, M., & Gouin, D. (2009). *Information Sharing Option Analysis* (External Client Report).

Breton, R. (2010). *Joint Command Decision Support for the 21st Century Technology Demonstration Project: Lessons Learned from experiment, demonstration and training events.*

Breton, R., & Guitouni, A. (2009). *Data Analysis of Joint Command Decision Support - Pegasus Guardian Experiment 1* (Technical Report).

CAE (2008). *IR Manager - Federation Requirements* (Contractor Report).

CAE (2008). *IR Manager - Functional Requirements* (Contractor Report).

CAE (2008). *IR Manager - Security Requirements* (Contractor Report).

CAE (2008). *IR Manager- JCDS 21 Integration Requirements* (Contractor Report).

CAE (2008). *JCDS TDP TA21 IR Manager 3.8 - System Design Specification (SDS) Design Changes* (Contractor Report).

CAE (2009). Information Request Manager (Version 4.0.0) [Installation Disks].

CAE (2009). *Information Request Manager 4.0 - Configuration Plan* (Contractor Report).

CAE (2009). *Information Request Manager 4.0 - System Administrator Guide* (Contractor Report).

CAE (2009). *Information Request Manager 4.0 Software Installation Plan* (Contractor Report).

CAE (2009). *Information Request Manager (IRM) Administrator Training* (Power Point Presentation).

CAE (2009). *Information Request Manager (IRM) User Training* (PowerPoint Presentation).

CAE (2009). *IR Manager Federation Deployment - Test Plan* (Contractor Report).

CAE (2009). *IR Manager Federation Deployment - Test Report* (Contractor Report).

Carson, N., & Caron, J.-D. (2010). *Vancouver 2010 Olympics: Collateral Damage Considerations (not yet received)* (Letter report - S (CEO)).

Carson, N., & Caron, J.-D. (2010). *Vancouver 2010 Winter Olympics - Intercept and Engagement Platform Options Analysis (not yet received)* (Technical Memorandum).

Carson, N., Caron, J.-D., & Bourdon, S. (2009). *Vancouver 2010: Defence Against the Asymmetric Air Threat (not yet received)* (Scientific Literature - S).

Carson, N., Caron, J.-D., Bourdon, S., & de Jong, P. (2010). *Vancouver 2010 Winter Olympics - A Spatial and Temporal Analysis of the Asymmetric Air Threat (not yet received)* (Technical Report - S (CA/US Eyes Only)).

Cazzolato, F., Dooley, P. W., & Henderson, M. D. (2009). *Ex BLUE Magnetometer Sensitivity Tests: Preliminary Findings* (Power Point Presentation - PB).

Chouinard, P. (2008). *Briefing to the Office of the Coordinator for 2010 Olympics and G8 Security* (Power Point Presentation).

Chouinard, P. (2009). *Feedback on the Joint Emergency Liaison Committee (JELC) Data Collection Spreadsheet* (Letter Report).

Chouinard, P. (2009). *Overview of the V2010 Infrastructure Criticality Study* (Letter Report).

Chouinard, P., & Genik, L. (2009). *Vancouver 2010 Olympics Critical Infrastructure - Final Criticality Assessment* (Letter Report - PB).

Chouinard, P., Verga, S., & Baingo, D. (2009). *Vancouver 2010 Olympics Critical Infrastructure - Final Criticality Assessment* (Letter Report - S).

Coates, C., & Perlin, M. (2009). *Ergonomic and Layout Analysis of the Joint Task Force (Games) Operations Centre* (Contractor Report-PB).

Coates, C., Perlin, M., & Stewart, A. (2009). *Ergonomic and Layout Analysis of the Integrated Command Centre* (Contractor Report).

Couillard, M., & Saunders, P. *Vancouver 2010 Burrard Inlet Patrol Boat Requirements* (PowerPoint Presentation).

Couillard, M., & Saunders, P. (2010). *Vancouver 2010" Burrard Inlet Patrol Boat Requirements (not yet received)* (Letter Report).

Crowe, V. (2010). *MFP-TDP Canadian Underwater Protection System trials - September 14-30, 2009* (Letter Report).

Desharnais, F. *Options Analysis for the Waterside Security of the Olympic Village* (Letter Report - PB).

Desharnais, F. (2008). *Marine Security Technology Survey* (Letter Report).

Desharnais, F., Crowe, V., Hazen, M., Chaisson, S., Crawford, A., Labbe, J.-N., et al. (2010). *Options Analysis for Waterside Security (DRAFT - PB)* (External Client Report).

Dixson, M. (2008). *Analysis of Integrated Command Centre C2 Network Architecture Options - Results from the 9 May 2008 Video Teleconference* (Lettter Report).

Dixson, M., Funk, R., Allen, D., Desrosiers, M., Goodman, L., Gouin, D., et al. (2009). *Exercise Gold: DRDC Analysis Quick Look* (Letter Report - PB).

Dixson, M., & Genik, L. (2010). *Application of Command and Control Architecture Frameworks for Security and Emergency Management Planning*. Paper presented at the NATO MSG 082 Workshop, 3-5 May 2010.

Dixson, M., Genik, L., Baingo, D., & Bureaux, J. (2008). *DRDC Validation Support Team - Observations and Lessons Identified: Exercise Bronze* (Technical Note).

Dooley, P. W. (2007). *Vancouver 2010 Vehicle Search Area Process Model: Preliminary Development* (Power Point Presentation).

Dooley, P. W. (2008). *Mock Area Screening Exercise (Ex MOCKASIN) Quicklook Report 1* (Letter Report -PB).

Dooley, P. W. (2008). *PSA Calculator v3.1.2: A Tool for Best-Case V2010 Pedestrian Screening Area Estimates* (Letter Report - PB).

Dooley, P. W. (2008). *Simplified Ambient Air Heating Calculation* (Working Document).

Dooley, P. W. (2008). *Vancouver 2010 VISTA-VSA Model: Interim Development* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Exercise BLUE Analysis 1: Walk-Through Magnetometer Characterization* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Exercise BLUE Analysis 2: Pedestrian Screening Area Operations* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Instrument Configuration & Evaluation Exercise (Ex ICE): Quicklook Results* (Power Point Presentation - PB).

Dooley, P. W. (2010). *Aides-Memoire for V2010 Vehicle Screening Area Personnel* (14 Working Documents - PB).

Dooley, P. W. (2010). *Potential Planning Considerations for G8 and G20 Summits (Draft)* (Working Document - PB).

Dooley, P. W. (2010). *Science-Based Planning Support to Vancouver 2010 Security: Two Case Studies*. Paper presented at the Knowledge Systems for Coalition Operations 2010 Conference.

Dooley, P. W. (2010). *Vancouver 2010 Vehicle Screening Area Experimentation 1 - Mock Area Screening Exercise (Ex MOCKASIN)* (Draft Technical Report).

Dooley, P. W., Cazzolato, F., Drolet, F., Henderson, M. D., Keefe, A., Terhaar, P., et al. (2009). *Exercise Blue Analysis 1: Characterization of the Walk-Through Magnetometer Response* (Letter Report - PB).

Dooley, P. W., Dixson, M., Evans, J., & Naprstek, T. (2010). *Exercise Blue Analysis 3: Vehicle Screening Area Operations* (Letter Report - PB).

Dooley, P. W., Terhaar, P., Cazzolato, F., Drolet, F., Henderson, M. D., Keefe, A., et al. (2009). *Exercise Blue Analysis 2: Pedestrian Screening Area Operations* (Letter Report - PB).

Duncan, P., Lombardi, B., Saunders, P., & Zegers, A. (2008). *Force Protection Matrix Game - Marine One: Post-Game Observations* (Letter Report - PB).

EMBC (2009). *British Columbia Chemical, Biological, Radiologica, Nuclear and Explosives Terrorism Response Plan (DRAFT)* (Contractor Report).

Emergency Management BC (2010). Vancouver 2010 Integrated Connectivity Schematic. In EMBC_C2_V2010ConnectivitySchematic (Ed.).

Erhardt, L. S. (2009). *Canadian RN Deployment for Vancouver 2010 in Support of CBRN Security*. Paper presented at the NATO RNDSG Meeting.

Erhardt, L. S., Sparkes, S., Quayle, D., Ellaschuk, B., Kenny, P., Morris, R., et al. (2009). *Canadian Radiological Emergency Response Exercise Scenarios Using Both Sealed and Unsealed Radioactive Sources*. Paper presented at the 54th Annual Meeting of the Health Physics Society.

Fujitsu (2009). *Major Events Coordinated Security Solutions (MECSS) - Framework Options Analysis* (Contractor Report).

Fujitsu (2010). *IRM Deployment Options* (Contractor Report).

Fujitsu (2010). *IRM Deployment Recommendation* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - Functional Requirements V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Document Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Process Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Role Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Operational Task Analysis V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Work Plans V1.2* (Contractor Report).

Fujitsu (2010). *Sustaining and Evolving GC2.0 Internal Collaborative Tools* (Contractor Report).

Funk, R. (2008). *Observations on Pegasus Guardian II and the V2010 C2 Framework* (Power Point Presentation).

Funk, R. (2008). *V2010 Vehicle Search Area Capacity: Review of Modeling and Planning Assumptions* (Power Point Presentation - PB).

Funk, R. (2009). *Integrated Security Architecture Modeling and Process Mapping - Extract from Full Version* (Contractor Report).

Funk, R. (2010). *Adaptation of Research Methods to Support the Analysis of Inter-Agency Training*. Paper presented at the Knowledge Systems for Coalition Operations 2010.

Funk, R., Breton, R., & Maceda, E. (2008). *Initial Analysis of JTFG GJOC Pegasus Guardian 2 CPX During Ex Bronze in Richmond, BC* (Letter Report - PB).

Funk, R., & Dooley, P. W. (2008). *Quicklook Analysis of V2010 Vehicle Search Area Capacity based on VANOC Planning Assumptions* (Power Point Presentation - PB).

Funk, R., Zegers, A., Breton, R., & Hazen, M. (2009). *Initial Analysis of JTFG Participation in Pegasus Guardian 2.2 Command Post Exercise and Ex Silver at Richmond, BC* (Letter Report - PB).

Gauthier, Y., & Adamsson, J. (2010). *Modelling and Simulation Tools for Decision Support to Canada Command* (DRAFT Technical Report).

Gauthier, Y., & Gammon, M. (2009). *Analytical Support to Canada Command During Exercises Silver and Staunch Maple 09 (February 9-12, 2009)* (Letter Report).

Genik, L., & Lauder, M. (2009). *Analysis of Provincial Regional Operations Centre (PREOC) Operations During Exercise Silver February 9-12, 2009* (Letter Report).

Genik, L., Lauder, M., & Maceda, E. (2009). *Analysis of EMBC's South West Provincial Regional Operations Centre (PREOC) Operations during Exercise Gold* (Letter Report).

Gerber, J. D., Carson, N., & Caron, J.-D. (2010). *Analytic Visualization Tool (AVT) Vancouver 2010 Olympics Air Defence Case Study* (Contractor Report - S (CA/US Eyes Only)).

Goodman, L. (2009). *Analytical Support to the G8/G20 Integrated Security Unit During Exercises Trillium Sentry (December 8-10, 2009)* (Letter Report - PB).

Goodman, L. (2010). *Outbrief - Scientific Advisor to RCMP G8/G20 Sumits Integrated Security Unit* (Letter Report).

Gouin, D., & Trinh, K. (2008). *Battle Rhythm Requirements* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *TCC Layout Recommendations* (Letter Report - PB).

Gouin, D., & Trinh, K. (2008). *Theatre Command Centre - Bridge Layout Options* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *Theatre Command Centre Layout* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *Trip Report from Meeting with the ISU/JTFG - BattleRhythm* (Trip Report).

Guitouni, A. (2010). *C4ISR Mobile Lab Specs* (Power Point Presentation).

Hales, D. (2008). *Vancouver 2010 Olympic Security Unit: Concept of Operations Summary Presentation* (Power Point Presentation).

Hales, D., & Miller, J. (2008). *Vancouver 2010 Integrated Security - Command and Control Concept of Operations* (Contractor Report).

Hales, D., & Miller, J. (2008). *Vancouver 2010 Integrated Security: Command and Control Concept of Operations Narrative* (Contractor Report).

Hales, D., & Miller, J. (2010). *Vancouver 2010 Integrated Security Command and Control Architecture: Concept of Operations Stakeholders' Analysis and Narrative* (Contractor Report - PB).

Hales, D., Miller, J., & Poursina, S. (2009). *Integrated Security Architecture Modelling and Process Mapping: Analysis of Vancouver 2010 Olympics Integrated Security Process* (Contractor Report).

Hales, D., Miller, J., & Poursina, S. (2010). *Vancouver 2010 Integrated Security Command and Control Architecture - Modeling and Process Mapping* (Contractor Report - PB).

Hewitt, A. (2009). *LRAD Options Summary* (Letter Report).

Hewitt, A., & Crowe, V. (2009). *Maritime Force Protection TDP Underwater Component build 3 Trial SITREP* (Letter Report).

Hill, A. (2010). *Scheduling Days Off for Officers Working at the G8/G20 Meetings* (Letter Report - PB).

Hill, A. (2010). *Tool to Assist the G8/G20 Planners for Arrivals and Departures of Officers* (Letter Report).

Hill, A., & Kaluzny, B. L. (2009). *DRDC CORA SUPPORT TO VANCOUVER 2010 OLYMPICS: SCHEDULING OF INTEGRATED SECURITY UNIT PERSONNEL* (Letter Report - PB).

Hill, A., & Kaluzny, B. L. (2009). *SCHEDULING V2010-ISU SECURITY PERSONNEL: A CASE STUDY* (Letter Report - PB No. 3553-1 (DMGOR AST).

Hill, A., & Kaluzny, B. L. (2010). *Scheduling Security Personnel for Vancouver 2010 Olympic Venues* (Technical Report).

IBM (2009). *ILOG OPL Development Studio: Scheduling of Personnel Workshifts User Guide* (Contractor Report).

ISR (2008). *V2010 Federal CBRNE Capabilities* (Contractor Report).

ISR (2008). *Vancouver 2010 Olympics - V2010 Federal CBRNE Technical Assistance Team Concept of Operations* (Contractor Report).

ISR (2009). *BC First Responder CBRNE Refresher Course* (Power Point Presentation).

ISR (2009). *BC Mass Decontamination Concept of Operations (CONOPS)* (Contractor Report).

ISR (2009). *C2010 - Live CBRNE Exercises: Guide for Players* (Contractor Report).

ISR (2009). *CSS/MECSS V2010 CBRNE Sensor Suite Plan: Accommodation Vessels* (Contractor Report).

ISR (2009). *CSS/MECSS V2010 Gold Training and Exercise Plan* (Contractor Report).

ISR (2009). *Gold - CBRNE Exercises: Controller's Manual* (Contractor Report).

ISR (2009). *Gold Live CBRNE Exercises 2009: Source Management Plan* (Contractor Report).

ISR (2009). *V2010 BC CBRNE Capability Analysis: Part 1 - Summary and Gap Identification* (Contractor Report).

ISR (2009). *V2010 BC CBRNE Capability Analysis: Part II - Assessment Data* (Contractor Report).

ISR (2009). *V2010 CBRNE Tabletop Exercise (TTX) Concept of Operations (CONOPS)* (Contractor Report).

Jaurez, H., & Marti, J. R. (2009). *Case Study: Transportation & Treatment of BC Place Victims During V2010 Olympics* (Contractor Report).

Jones, T., & Larsson, C. L. (2010). *Training Workshop on the Sensitive Directional Gamma-Ray Probe* (Power Point Presentation).

Jong, P. d. (2009). *Exercise Silver TPS-70 Electromagnetic Interference Problem: An OR Perspective* (Letter Report).

Kaluzny, B. L., & Hill, A. (2010). Scheduling Security Personnel for the Vancouver 2010 Winter Olympic Games. [DRAFT Journal Article]. *Journal of Scheduling*.

Kaluzny, B. L., & Hill, A. (2010). *Security Scheduling and a Qualitative MCDA Method (not yet received)* (Powerpoint Presentation).

Karthaus, C. L. F., Hall, C. D. T., & Martin, L. B. (2009). *Analysis of Collaboration Among Operational Teams Involved in Security During the Vancouver 2010 Olympic Games* (Contractor Report - PB).

Keefe, A., Lamb, M., Terhaar, P., Au, H., & Maceda, E. (2009). *Human Factors Issues Affecting Security Personnel Working at the Vehicle Screening Areas (VSA) and Pedestrian Screening Areas (PSA)* (Letter Report - PB).

Khouj, M. T., & Marti, J. R. (2010). *Modeling Critical Infrastructure Interdependencies in Support of the Security Operations for the Vancouver 2010 Olympics* (Technical Report).

Larsson, C. L. (2009). *Canadian Radiological Field Exercise*. Paper presented at the ITWG Nuclear Forensic Laboratories Meeting.

Larsson, C. L. (2009). *Radiological and Nuclear Terrorism Overview for the vancouver Police Department Radiological Roensic Exercise Training (Power Point Presentation)* (Power POint Presentation).

Larsson, C. L. (2010). *Radiological and Nuclear Detection Architecture for V2010*. Paper presented at the STIG Meeting.

Lauder, M. (2009). *2010 Adversary Survey and Supplemental Analysis* (Letter Report - C).

Lauder, M. (2009). Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces. *Canadian Forces' Canadian Army Journal, 12.2*, 25-36.

Lauder, M. (2009). *Red Teaming the Red Team: Out-brief of the Adversarial Intent Workshop, 09-11 June 2009, CFB Esquimalt* (Letter Report - C).

Lauder, M., McIntyre, S., Zegers, A., & Funk, R. (2010). *Exercise Laurel Wreath 1001 Results for Games Red Team* (Letter Report - PB).

Lauder, M. A. (2009). *Emulating the Adversary: Red Teaming and Threat Reduction*. Paper presented at the 2009 Canadian Association for Security Intelligence Studies (CASIS) Conference.

Lauder, M. A. (2010). *CHINYAVADA CELL: Recalibrating the Generated Threat for Application by the Games Red Team, Joint Task Force Games* (Letter Report - C).

Lavigne, S., Kitching, F., McCall, M., & Sykes, T. (2009). *V2010 CBRNE Tabletop Exercise 2009 (TTX-09): After Action Report* (Technical Note).

Lavigne, S., Morris, R., McCall, M., & Sykes, T. (2009). *V2010 CBRNE Live Play Exercise 2009: After Action Report* (Contractor Report - PB).

Lavigne, S., Nguyen, T., McCall, M., & Sykes, T. (2009). *Exercise Initial Thunder 2008: After Action Report* (Technical Note).

Lee, J. J. (2008). *Underwater Explosion Threat Assessment for the False Creek Inlet in the Athlete's Olympic Village* (Letter Report - PB).

Lemyre, L. (2008). *Orientation Notes on Evidence-based Guidance For Promoting Psychosocial Preparedness* (Letter Report).

Martec (2009). *Approach Report for BC/GMP and Athletes' Village Blast Modeling* (Contractor Report - S).

Martec (2009). *CSS Support - Site 1 Report: Summary of BC/GM Place Modelling Results* (Contractor Report - S).

Martec (2009). *CSS Support - Site 2 Report: Summary of Athlete's Village Modeling Results* (Contractor Report - S).

Martec (2009). *Large Scale Facility Modeling - BC Place Roof Analysis* (Contractor Report - S).

Marti, J. R. (2009). *I2Sim to Support CoV Emergency Response* (Contractor Report).

Marti, J. R. (2009). *Vulnerabilities and Mitigation Strategies: Downtown Vancouver, 2010* (Contractor Report).

Masys, A. (2009). *Exercise Gold After Action Report: National Operations Centre (NOC)* (Letter Report - PA).

Masys, A., MacLatchy, J., Murray, C., & Wood, D. (2009). *Major Events Safety and Security Framework: A 'Whole of Government' approach to integrated planning*. Paper presented at the CRHNET.

Masys, A. J., Belanger, M., Gouin, D., & Wood, D. (2009). *National Operations Centre (NOC) Table-Top Exercise (TTX): After Action Report* (Letter Report - PB).

Maxwell, D., Silva, D. D., Shubaly, D., & Ltd., M. S. (2010). *Underwater Component Support for OP PODIUM (DRAFT)* (Contractor Report).

McIntyre, S. (2008). *CAPEX08: Lessons Learned* (Letter Report - PB).

McLellan, T., & Paul, M. (2010). *Guidance for Heat Stress and Sleep for G8/G20* (Power Point Presentation).

Mitrovic-Minic, S., Guitouni, A., & Zwick, H. (2010). *Risk Aggregation Methodology for Emergency Management*. Paper presented at the FIRST REGIONAL CONFERENCE OF THE EUROPEAN DECISION SCIENCES INSTITUTE.

Morris, R., McCall, M., Sykes, T., & Thompson, C. (2008). *Exercise Integrated Response 2008 (ExIR-08): After Action Report* (Technical Note).

Nadeau, C., & Wood, S. (2009). *Major Events Security Framework: Information Sharing and Knowledge Management Final Report* (Contractor Report).

Pourian, I. (2009). *New Thinking on Major Event Safety and Security* (Contractor Report).

Quayle, D. (2009). *Observations on the Employment of CBRN Scientific Advisors in Support of the National CBRNE Response Team During Exercise Silver Febrary 9-12, 2009* (Letter Report - PB).

Reedel, G., & Nadeau, C. (2009). *Development of an Ontology in Support of JCDS 21 Final Report* (Contractor Report).

Rehak, L., McDermott, K., Famewo, J., & Martin, L. B. (2008). *Final Synthesis Report for Social Network Analysis of Joint Interagency Multinational & Public (JIMP) Operations* (Contractor Report).

Sand, B. (2010). *Joint Task Force Games Vancouver 2010 Winter Olympics Games Red Team: Final Report* (Letter Report).

Smith, D., Allen, D., Dooley, P. W., Hawton, A., & Pavlovic, N. (2008). *Initial Analysis of ISU Theatre Command Centre (TCC) Operations During Exercise Pegasus Guardian II (November 12-14, 2008)* (Letter Report - PB).

Smith, D., Allen, D., Hawton, A., & Dixson, M. (2009). *Initial Analysis of ISU Theatre Command Centre (TCC) Operations During Exercise Pegasus Guardian 2-2 and Exercise Silver (February 2-12, 2009)* (Letter Report - PB).

Smith, D., & Chow, R. (2008). *Analysis of Responses to the OMOC Information Sharing Questionnaire* (Letter Report).

Smith, D., Genik, L., Maceda, E., & Masys, A. (2010). *Vancouver 2010 PREOC Operations Report* (Letter Report).

Smith, D., & Maceda, G. E. (210). *Strategies for ad-hoc Data Collection and Analysis During major Event Interagency Exercises and Operations*. Paper presented at the Knowledge Systems for Coalition Operations 2010.

Steele, J. (2009). *On Observations and Assessment of Joint Interface Control Cell (JICC) Operations During Ex Staunch Maple* (Letter Report - S).

Steele, J. (2010). *On CF Tactical Data Link Capability Development* (Letter Report).

Sykes, T. (2010). Science Town Fact Sheet English.

Sykes, T. (2010). Science Town Fact Sheet French.

Verga, S., Chouinard, P., & Baingo, D. (2008). *The Critical Infrastructure Asset Ordination (CIAO) Model* (Technical Memorandum).

Wang, W. (2009). *Joint Command Support through Workspace Analysis, Design and Optimization* (Technical Report).

Wood, D. (2009). *Analysis Report Pegasus Guardian III - NOC Observations* (Letter Report - PB).

xwave (2009). Information Request Manager (Version 3.8.0) [Source Code].

Yee, E. (2010). *An Operational Implementation of a CBRN Sensor-Driven Modeling paradigm for Stochastic Event Reconstruction: Technical Description of an Advanced Modeling Component of CRTI PRoject 07-0196TD (DRAFT)* (Technical Report).

Yee, E., Lien, F.-S., & Ji, H. (2010). *A Building-Resolved Wind Field Library for Vancouver: Facilitating CBRN Emergency Response for the 2010 Winter Olympic Games (DRAFT)* (Technical Memorandum).

Zegers, A. (2008). *Trip Report to Force Protection Matrix Game Darwin Australia - 23-30 June 2008* (Trip Report).

Zegers, A. (2009). *Analysis of OMOC Participation in Exercise Gold* (Letter Report - PB).

Zegers, A. (2010). *Matrix Game Methodology Development and Employment for Vancouver 2010 Olympics Marine Security Planning* (Scientific Literature).

Zegers, A. (2010). *Matrix Game Methodology: Support to V2010 Olympic Marine Security Planners* (Technical Report).

Zegers, A., & Hazen, M. (2009). *Analysis of OMOC Participation in Exercise Pegasus Guardian 3* (Letter Report - PB).

Zegers, A., & Saunders, P. (2008). *Force Protection Matrix Game - Marine Two: After Action Report* (Letter Report - PB).

Zegers, A., Saunders, P., Rudd, D., & Sand, M. B. (2009). *Integrated Safety/Security Matrix Game - Marine III: After Action Report* (Letter Report - PB).

This page intentionally left blank.

List of Acronyms

ACC	Air Command Centre
ADM	Assistant Deputy Minister
ADM EMC	Assistant Deputy Minister Emergency Management Committee
AER	After Event Review
ASIA	Automated Ship Image Acquisition
AWAND	Alternate Workspace Analysis and Design
C2	Command and Control
C3IS	Command, Control, Communications and Information Systems
C4ISR	Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance
CATSA	Canadian Air Transport Security Authority
CATSI	Compact Atmospheric Sounding Interferometer Engineering Development Model
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CCIRC	Canadian Cyber Incident Response Centre
CERL	Canadian Explosives Research Laboratory
CF	Canadian Forces
CF LO	Canadian Forces Liaison Officer
CFEC	Canadian Forces Experimentation Centre
CFEWC	Canadian Forces Electronic Warfare Centre
CI	Critical Infrastructure
CICI	Critical Infrastructure Criminal Intelligence
CID	Criminal Intelligence Directorate
CIP	Criminal Intelligence Program
CIS	Communications Information System
CONAF	Confirmation Architecture Framework
CONOPS	Concept of Operations
COO	Chief Operating Officer
CORA	Centre for Operations Research and Analysis
CoV	City of Vancouver
CPX	Command Post Exercise

CRTI	Chemical, Biological, Radiological, Nuclear, Explosives, Research Technology Initiative
CSNI	Canadian Secure Network Infrastructure
CSS	Centre for Security Science
DANTE	Data Acquisition via Netbook Tablet Entry
DGNS	Director General Nuclear Safety
DLSE	Directorate Land Synthetic Environment
DM SAC	Deputy Minister Security Advisory Committee
DND	Department of National Defence
DNDAF	Department of National Defence Architecture Framework
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
EMBC	Emergency Management British Columbia
EX	Exercise
EXP	Experiment
FPMG	Force Protection Matrix Game
GIS	Geographical Information System
GJOC	Games Joint Operations Centre (CF)
GOC	Government Operations Centre
GRT	Joint Task Force Games Red Team
HQ	Headquarters
IBET	Integrated Border Enforcement Team
IC	Industry Canada
IP	Intellectual Property
IR Mgr	Information Request Manager
ISU	Integrated Security Unit
JCC	Joint Command Centre
JCDS 21	Joint Command Decision Support for the 21st Century
JELC	Joint Emergency Liaison Committee
JICC	Joint Interface Control Cell
JTFG	Joint Task Force Games
JTFP	Joint Task Force Pacific

LRAD	Long Range Acoustic Device
LW	Laurel Wreath
MARPAC	Maritime Pacific
MCC	Maritime Command Centre
MECSS	Major Events Coordinated Security Solutions
MESF	Major Events Security Framework
ME&PS	Major Events and Protective Services
MFP TDP	Maritime Force Protection Technology Demonstration Project
N CBRNE RT	National CBRNE Response Team
NCS	National Communication Services
NCR	National Capital Region
NDA	Non-Disclosure Agreement
NIO	Network Information Operations
NOC	National Operations Centre
NSERC	National Science and Engineering Research Council
OCS	Office for the Coordinator for the Security of the Olympics and G8
OMOC	Olympic Marine Operations Centre
ORT	Operations Research Team
PCO	Privy Council Office
PEP	Provincial Emergency Program
PIDS	Perimeter Intrusion Detection System
PG	Pegasus Guardian
PREOC	Provincial Regional Emergency Operations Centre
PS	Public Safety
PSA	Pedestrian Screening Area
PSTP	Public Security Technical Program
PSU	Property Security Unit
RCMP	Royal Canadian Mounted Police
RVSS	Remote Vehicle Screening Site
R&D	Research and Development

SA	Scientific Advisor
SME	Subject Matter Expert
SOPs	Standard Operating Procedures
SRB	Senior Review Board
S&T	Science and Technology
TCC	Theatre Command Centre
TD	Technology Demonstration
TTCP	The Technical Cooperation Panel
TTX	Table Top Exercise
UBC	University of British Columbia
V2010	Vancouver 2010 Winter Olympics and Paralympics
VACC	Vancouver Area Command Centre
VANOC	Vancouver Organizing Committee for the 2010 Olympic and Paralympic Winter Games
VFD	Vancouver Fire Department
VPD	Vancouver Police Department
VSA	Vehicle Screening Area
WACC	Whistler Area Command Centre

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Centre for Security Science (CRTI/PSTP)
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Major Events Coordinated Security Solutions Technical Report Closeout: The Application of Science and Technology to Reduce Risk for V2010 and G8/G20 Summits

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Murray, C.; Wood, D.; MacLatchy, J; Chouinard, P; Dixson, M; Dooley, P; Funk, R; Genik, L; Guitouni, A; Masys, T; Sykes, T

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2010	82	0

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science (CRTI/PSTP)
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
32bj	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TR 2010-13	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The Major Events Coordinated Security Solutions (MECSS) project was a multi-agency collaborative partnership established to reduce the security risk associated with V2010 and the G8/G20 Summits. Decision Support, Exercise Support, Reach-back scientific advice and deployed support during the V2010 and Summits was provided in Command and Control, Chemical Biological, Radiological, Nuclear and Explosives, Critical Infrastructure, Surveillance, Physical Security, Cyber and Psycho-Social. This technical report constitutes the closeout report for the MECSS project and provides a summary of the results achieved by MECSS.

Le projet Solutions concertées pour la sécurité des grands événements (SCSGE) était un partenariat de collaboration multi-organismes, mis en place afin d'atténuer les risques pour la sécurité des Jeux olympiques d'hiver de Vancouver 2010 et des sommets du G8 et du G20. Il a permis de fournir l'aide à la décision, le soutien des exercices, les conseils scientifiques extérieurs et le soutien aux opérations de déploiement durant les Jeux olympiques et ses sommets dans les domaines connexes au commandement et contrôle, aux incidents chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRNE), aux infrastructures essentielles, à la surveillance, à la sécurité physique, à la cybernétique et à la socio-psychologie. Le présent rapport technique clôture le projet SCSGE et fournit un résumé des résultats atteints

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

V2010; G8/G20; Major Events; security; Olympics; Critical Infrastructure; CBRNE; Command and Control; Surveillance; VSA; Exercises;